Microsoft

Microsoft Digital Defense Report 2022

Zur Beleuchtung der Bedrohungslandschaft und Unterstützung einer digitalen Verteidigung

Inhaltsverzeichnis

Sofern nicht anderweitig angegeben, stammen die Daten, Befunde und Ereignisse in diesem Bericht aus den Monaten Juli 2021 bis einschließlich Juni 2022 (Microsoft-Geschäftsjahr 2022).

Um die bestmögliche Erfahrung beim Anzeigen und Navigieren dieses Berichts zu erhalten, empfehlen wir die Verwendung von Adobe Reader. Er steht als kostenloser Download auf der Adobe-Website zur Verfügung.

Einführung von Tom Burt

Corporate Vice President, Customer Security & Trust

„Anhand der Analyse von Billionen Signalen aus unserer weltweiten Infrastruktur von Produkten und Diensten erhalten wir Aufschluss über die Intensität, den Umfang und die Größenordnung digitaler Bedrohungen auf der ganzen Welt.“

Eine Momentaufnahme unserer Landschaft ...

Umfang und Größenordnung der Bedrohungslandschaft

Das Volumen der Kennwortangriffe ist auf schätzungsweise 921 Angriffe pro Sekunde gestiegen – ein Anstieg um 74 % in nur einem Jahr.

Entschärfen von Cyberkriminalität

Bis heute hat Microsoft mehr als 10.000 Domänen von Cyberkriminellen und 600 von nationalstaatlichen Akteuren entfernt.

Behebung von Schwachstellen

Bei 93 % unserer Initiativen für die Reaktion auf Ransomware-Vorfälle zeigten sich unzureichende Kontrollen über privilegierte Zugriffsberechtigungen und laterale Bewegungen.

Am 23. Februar 2022 begann für die Welt der Cybersicherheit ein neues Zeitalter: das Zeitalter der hybriden Kriegsführung. An diesem Tag, Stunden bevor die ersten Raketen abgefeuert wurden und Panzer über die Grenzen rollten, haben russische Akteure eine massive zerstörerische Cyberattacke gegen Ziele in der ukrainischen Regierung sowie im ukrainischen Technologie- und Finanzsektor gestartet. Weitere Informationen zu diesen Angriffen und den daraus gelernten Lektionen finden Sie im Kapitel „Bedrohungen durch Nationalstaaten“ dieser dritten Ausgabe des jährlichen Microsoft Digital Defense Report (MDDR). Eine der wichtigsten Erkenntnisse ist, dass die Cloud den besten physischen und logischen Schutz vor Cyberangriffen bietet und Fortschritte bei Threat Intelligence und Endpunktschutz ermöglicht, die ihren Wert in der Ukraine unter Beweis gestellt haben.

Während jede Analyse der Entwicklungen des vergangenen Jahres dort ihren Ausgangspunkt nehmen muss, liefert der diesjährige Report auch tiefe Einblicke in viele weitere Sicherheitsthemen und -aspekte. Im ersten Kapitel des Berichts konzentrieren wir uns auf Aktivitäten von Cyberkriminellen, gefolgt von Bedrohungen durch Nationalstaaten in Kapitel 2. Beide Gruppen haben die Komplexität ihrer Angriffe stark erhöht, was eine drastisch stärkere Wirkung ihrer Aktionen zur Folge hat. Während Russland die Schlagzeilen beherrschte, eskalierten iranische Akteure ihre Angriffe nach einem Wechsel der Präsidentschaft. Sie starteten zerstörerische Angriffe auf Israel sowie Ransomware- und Hack-and-Leak-Aktionen gegen kritische Infrastruktur in den USA. Auch China hat seine Spionageaktivitäten in Südostasien und anderswo im globalen Süden ausgedehnt, um dem Einfluss der USA entgegenzuwirken und an kritische Daten und Informationen zu gelangen.

Ausländische Akteure setzen außerdem hochwirksame Techniken ein, um Propagandamaßnahmen in vielen Ländern weltweit zu befördern. Das ist Gegenstand des dritten Kapitels. Russland hat beispielsweise großen Aufwand betrieben, um seine Bürger sowie die Bürger vieler anderer Länder davon zu überzeugen, dass der Angriff auf die Ukraine gerechtfertigt war. Gleichzeitig säte es Propaganda zur Diskreditierung der COVID-Impfstoffe des Westens, während die Wirksamkeit der eigenen Entwicklungen stark übertrieben wurde. Darüber hinaus zielen die Akteure zunehmend auf Geräte des Internets der Dinge (Internet of Things, IoT) oder auch auf OT-Steuergeräte ab, da diese als Zugriffspunkte für Netzwerke und kritische Infrastruktur dienen. Dieses Thema wird in Kapitel 4 behandelt. Im letzten Kapitel präsentieren wir schließlich Insights und Lektionen, die wir im Laufe des letzten Jahres bei der Verteidigung gegen Angriffe auf Microsoft und unsere Kunden gelernt haben. Dabei werfen wir einen näheren Blick auf die Entwicklungen bei der Cyberresilienz.

Jedes Kapitel behandelt die wichtigsten Lektionen und Insights, wie sie sich aus der umfassenden Perspektive von Microsoft darstellen. Anhand der Analyse von Billionen Signalen aus unserer weltweiten Infrastruktur von Produkten und Diensten erhalten wir Aufschluss über die Intensität, den Umfang und die Größenordnung digitaler Bedrohungen auf der ganzen Welt. Microsoft ergreift Maßnahmen, um unsere Kunden und die digitale Infrastruktur gegen diese Bedrohungen zu verteidigen. Sie erfahren außerdem mehr über unsere Technologie zum Identifizieren und Blockieren von Milliarden von Phishing-Versuchen, Identitätsdiebstählen und anderen Bedrohungen gegen unsere Kund*innen.

Einführung von Tom Burt

Fortsetzung

Wir setzen auch rechtliche und technische Mittel ein, um die von Cyberkriminellen und nationalstaatlichen Akteuren genutzte Infrastruktur zu beschlagnahmen und abzuschalten. Des Weiteren benachrichtigen wir Kund*innen, wenn sie von einem nationalstaatlichen Akteur bedroht oder angegriffen werden.
Wir arbeiten daran, immer effektivere Funktionen und Dienste zu entwickeln, die Cyberbedrohungen mithilfe von KI-/ML-Technologie identifizieren und blockieren, und Sicherheitsexpert*innen werden bei der Erkennung und Bekämpfung von Cyberangriffen immer schneller und effektiver.

Am wichtigsten ist vielleicht, dass wir im gesamten MDDR unsere besten Tipps zu den Maßnahmen geben, die Einzelpersonen, Organisationen und Unternehmen ergreifen können, um sich vor diesen zunehmenden digitalen Bedrohungen zu schützen. Die Einführung guter Praktiken der Cyberhygiene ist die beste Verteidigung und kann das Risiko von Cyberattacken deutlich reduzieren.

Lagebericht zur Cyberkriminalität

Cyberkriminelle agieren weiterhin als raffinierte Profitunternehmen. Angreifer passen sich an und finden neue Wege zum Implementieren ihrer Techniken. Dabei werden sie bei Auswahl von Technik und Standort der Infrastruktur für die Durchführung ihrer Kampagnen immer komplexer. Gleichzeitig werden Cyberkriminelle immer sparsamer. Zur Senkung ihrer Betriebskosten und Steigerung der Legitimierung nach außen kompromittieren Angreifer Unternehmensnetzwerke und -geräte zum Hosten ihrer Phishing-Kampagnen und Schadsoftware oder sogar zur Nutzung der Rechenleistung für das Minen von Kryptowährung.

Weitere Informationen finden Sie auf S. 6

„Mit dem Einsatz von Cyberwaffen im hybriden Krieg in der Ukraine bricht ein neues Konfliktzeitalter an."

Bedrohungen durch Nationalstaaten

Nationalstaatliche Akteure führen immer ausgefeiltere Cyberattacken durch, die darauf ausgelegt sind, eine Erkennung zu umgehen und ihre strategischen Prioritäten voranzutreiben. Mit dem Einsatz von Cyberwaffen im hybriden Krieg in der Ukraine bricht ein neues Konfliktzeitalter an. Russland hat seinen Krieg auch mit Operationen zur Informationsbeeinflussung flankiert.
Dabei nutzte es Propaganda zur Beeinflussung von Meinungen in Russland, der Ukraine und weltweit. Außerhalb der Ukraine haben nationalstaatliche Akteure ihre Aktivität ausgeweitet und damit begonnen, technologische Fortschritte bei Automatisierung, Cloud-Infrastruktur und Remote-Zugriff für Angriffe auf eine breitere Palette von Zielen auszunutzen. Häufiges Angriffsziel waren IT-Lieferketten von Unternehmen, die einen Zugriff auf die letztendlichen Ziele ermöglichten. Cyberhygiene wurde noch wichtiger, weil die Akteure ungepatchte Schwachstellen schnell ausnutzten, sowohl ausgefeilte als auch Brute-Force-Techniken nutzten, um Anmeldeinformationen zu stehlen, und ihre Aktionen mithilfe von Open Source oder legitimer Software verschleierten. Darüber hinaus verbündet sich der Iran bei der Nutzung destruktiver Cyberwaffen mit Russland. Das schließt auch Ransomware als Grundpfeiler ihrer Angriffe mit ein.

Diese Entwicklungen erfordern die dringende Einführung eines einheitlichen, globalen Rahmens, der die Menschenrechte priorisiert und Menschen vor rücksichtslosem staatlichen Verhalten im Cyberraum schützt. Alle Nationen müssen zusammenarbeiten, um Normen und Regeln für ein verantwortungsvolles staatliches Verhalten zu implementieren.

Weitere Informationen finden Sie auf S. 30

Geräte und Infrastruktur

In Kombination mit der schnellen Einführung von Internetgeräten aller Art als eine Komponente zur Beschleunigung der digitalen Transformation hat die Pandemie die Angriffsfläche unserer digitalen Welt stark erhöht. Cyberkriminelle und Nationalstaaten nutzen das schnell aus. Obwohl die Sicherheit von IT-Hardware und -Software in den letzten Jahren robuster geworden ist, konnte die Sicherheit von IoT- und OT-Geräten nicht damit Schritt halten. Akteure etablieren über solche Geräte Zugriff auf Netzwerke und ermöglichen laterale Bewegung, wodurch sie in einer Lieferkette Fuß fassen oder die OT-Abläufe der Zielorganisation stören können.

Weitere Informationen finden Sie auf S. 56

Einführung von Tom Burt

Fortsetzung

Einflussnahme im Cyberspace

Nationalstaaten nutzen zunehmend ausgeklügelte Operationen zur Einflussnahme, um Propaganda zu streuen und die öffentliche Meinung sowohl im Inland als auch international zu beeinflussen. Diese Kampagnen untergraben Vertrauen, erhöhen die Polarisierung und bedrohen demokratische Prozesse. Erfahrene Akteure, die sich als Advanced Persistent Manipulators betätigen, nutzen traditionelle Medien zusammen mit dem Internet und Social Media, um den Umfang, die Größenordnung und die Effizienz ihrer Kampagnen und deren außerordentliche Auswirkungen auf die weltweiten Informationsnetzwerke enorm zu steigern. Im vergangenen Jahr wurden wir Zeugen, wie solche Operationen als Teil der russischen hybriden Kriegsführung in der Ukraine eingesetzt wurden. Wir erlebten aber auch, wie Russland und andere Nationen wie China und Iran in zunehmendem Maße von Social Media gestützte Propagandaaktionen durchführen, um ihren weltweiten Einfluss bei einer Vielzahl von Themen auszubauen.

Weitere Informationen finden Sie auf S. 71

Cyberresilienz

Sicherheit ist ein wichtiger Faktor für technologischen Erfolg. Innovation und gesteigerte Produktivität lassen sich nur durch die Einführung von Sicherheitsmaßnahmen erreichen, mit denen Unternehmen so resilient wie möglich gegen moderne Angriffe werden. Die Pandemie hat uns bei Microsoft vor die Herausforderung gestellt, unsere Sicherheitsmethoden und -technologien neu auszurichten, um unsere Mitarbeiter*innen zu schützen, egal, wo sie tätig sind. In diesem vergangenen Jahr haben Akteure weiterhin die während der Pandemie und des Umstiegs auf eine hybride Arbeitsumgebung zutage getretenen Schwachstellen ausgenutzt. Seitdem liegt unsere Herausforderung in erster Linie darin, auf die Verbreitung und Komplexität verschiedener Angriffsmethoden und die verstärkte Aktivität von Nationalstaaten zu reagieren. In diesem Kapitel gehen wir detailliert auf die Herausforderungen ein, denen wir gegenüberstanden, sowie auf die Verteidigungsmaßnahmen, die wir im Gegenzug mit unseren mehr als 15.000 Partnern mobilisiert haben.

Weitere Informationen finden Sie auf S. 86

Unsere einzigartige Perspektive

37 Mrd.
blockierte E-Mail-Bedrohungen

34,7 Mrd.
blockierte Identitätsbedrohungen

43 Bio.
täglich synthetisierte Signale mit ausgefeilten Datenanalysen und KI-Algorithmen, um digitale Bedrohungen und kriminelle Cyberaktivitäten nachzuvollziehen und sich davor zu schützen.

2,5 Mrd.
analysierte Endpunktsignale täglich

Über 8.500
Ingenieur*innen, Forschende, Datenwissenschaftler*innen, Cyberexpert*innen, Threat-Hunter, geopolitische Analyst*innen, Ermittler*innen und Frontline-Responder in 77 Ländern.

Mehr als 15.000
Partner in unserer Sicherheitsinfrastruktur, die die Cyberresilienz unserer Kunden verbessern.

1. Juli 2021 bis 30. Juni 2022

Einführung von Tom Burt

Fortsetzung

Wir sind überzeugt, dass Microsoft – unabhängig und durch enge Partnerschaften mit anderen aus Privatwirtschaft, öffentlicher Verwaltung und Zivilgesellschaft – die Verantwortung hat, die digitalen Systeme, die das Rückgrat unseres Sozialgefüges sind, zu schützen und sichere sowie geschützte Computerumgebungen für alle losgelöst vom Standort zu fördern. Diese Verantwortung ist der Grund, warum wir den MDDR seit 2020 jedes Jahr herausgeben. Dieser Bericht ist die Kulmination der umfangreichen Daten und der ausgedehnten Forschung von Microsoft. Er vermittelt unsere einzigartigen Insights darüber, wie sich die digitale Bedrohungslandschaft entwickelt und welche entscheidenden Maßnahmen heute ergriffen werden können, um die Sicherheit der Infrastruktur zu verbessern.

Wir hoffen, ein Gefühl der Dringlichkeit zu vermitteln, damit die Leser*innen anhand der von uns hier und in unseren zahlreichen Publikationen zur Cybersicherheit über das Jahr hinweg präsentierten Daten und Insights sofort Maßnahmen ergreifen können. Angesichts des Ernstes der Bedrohung für die digitale Landschaft – und ihrer Auswirkungen auf die physische Welt – darf nicht vergessen werden, dass wir alle Maßnahmen ergreifen können, um uns, unsere Organisationen und unsere Unternehmen vor digitalen Bedrohungen zu schützen.

Vielen Dank, dass Sie sich die Zeit nehmen, den diesjährigen Microsoft Digital Defense Report zu lesen. Wir hoffen, dass Sie wertvolle Insights und Empfehlungen daraus ziehen, damit wir alle unsere digitale Infrastruktur emeinsam verteidigen können.

Tom Burt
Corporate Vice President,
Customer Security & Trust

Wir verfolgen mit diesem Bericht zwei Ziele:

1. Die Beleuchtung von Entwicklungen in der digitalen Bedrohungslandschaft für unsere Kund*innen, Partner und Stakeholder in der breiter gefassten Infrastruktur, indem wir neue Cyberangriffe und aufkommende Trends bei historisch persistenten Bedrohungen betrachten
2. Die Unterstützung unserer Kund*innen und Partner bei der Verbesserung ihrer Cyberresilienz

Lagebericht zur Cyberkriminalität

Angesichts der immer besseren Cyberverteidigung und der proaktiven Herangehensweise von zunehmend mehr Organisationen bei der Verteidigung passen die Angreifer ihre Techniken an.

Übersicht über den

Stand der Cyberkriminalität

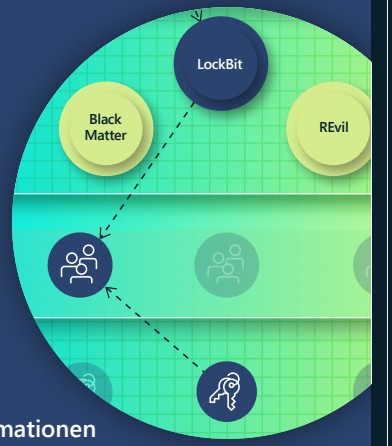
Angesichts der immer besseren Cyberverteidigung und der proaktiven Herangehensweise von zunehmend mehr Organisationen bei der Verteidigung passen die Angreifer ihre Techniken an.

Cyberkriminelle agieren weiterhin als raffinierte Profitunternehmen. Angreifer passen sich an und finden neue Wege zum Implementieren ihrer Techniken. Dabei werden sie bei Auswahl von Technik und Standort der Infrastruktur für die Durchführung ihrer Kampagnen immer komplexer. Gleichzeitig werden Cyberkriminelle immer sparsamer. Zur Senkung ihrer Betriebskosten und Steigerung der Legitimierung nach außen kompromittieren Angreifer Unternehmensnetzwerke und -geräte zum Hosten ihrer Phishing-Kampagnen und Schadsoftware oder sogar zur Nutzung der Rechenleistung für das Minen von Kryptowährung.

Cyberkriminalität nimmt weiter zu, weil die Industrialisierung der kriminellen Cyberwirtschaft durch immer besseren Zugang zu Tools und Infrastruktur weniger Fähigkeiten für den Einstieg erfordert.

Weitere Informationen finden Sie auf S. 18

Die Bedrohung durch Ransomware und Erpressung nimmt mit Angriffen auf Regierungen, Unternehmen und kritische Infrastruktur an Aggressivität zu.

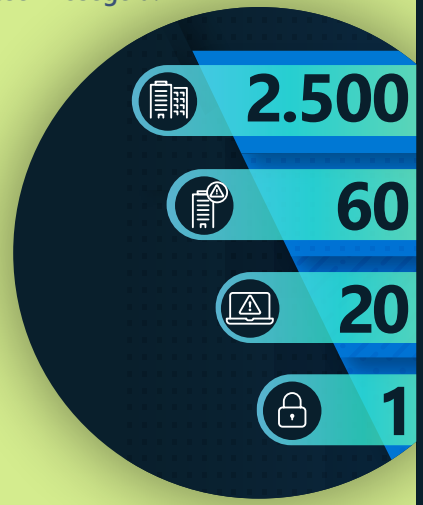


Weitere Informationen finden Sie auf S. 9

Angreifer drohen immer mehr mit der Offenlegung sensibler Daten, um Lösegeld zu erpressen.

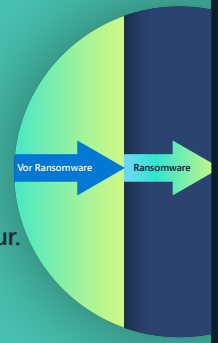
Weitere Informationen finden Sie auf S. 10

Von Menschen platzierte Ransomware ist die am weitesten verbreitete Variante. Ein Drittel der Ziele werden von Kriminellen kompromittiert, die diese Angriffe verwenden, und 5 % davon erpressen Lösegeld.



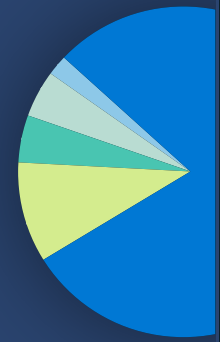
Weitere Informationen finden Sie auf S. 9

Zur den wirksamsten Verteidigungsmöglichkeiten gegen Ransomware zählen die Multi-Faktor-Authentifizierung, regelmäßige Sicherheitspatches und Zero Trust-Prinzipien für die gesamte Netzwerkarchitektur.



Weitere Informationen finden Sie auf S. 13

Phishing nach Anmeldeinformationen, das wahllos alle Posteingänge anvisiert, nimmt weiter zu. Die Kompromittierung geschäftlicher E-Mail-Konten, einschließlich Rechnungsbetrug, stellt ein erhebliches Cybercrimerisiko dar.



Weitere Informationen finden Sie auf S. 21

Bei der Zerschlagung bösartiger Infrastrukturen von Cyberkriminellen und nationalstaatlichen Akteuren setzt Microsoft auf innovative rechtliche Ansätze und unsere öffentlichen und privaten Partnerschaften.

Weitere Informationen finden Sie auf S. 25

Einführung

Cyberkriminalität nimmt weiter zu, mit Zuwachsraten bei sowohl zufälligen als auch gezielten Angriffen.

Da die Verteidigung gegen Cyberangriffe immer besser wird und zunehmend mehr Regierungen und Unternehmen einen proaktiven Präventivansatz wählen, sehen wird, dass Angreifer vor allem zwei Strategien nutzen, um sich den benötigten Zugriff zur Durchführung von Cyberverbrechen zu verschaffen. Ein Ansatz besteht in einer Kampagne mit weit gefächerten Zielen. Dabei setzen die Angreifer auf die reine Menge. Der andere setzt auf Beobachtung und eine selektivere Zielauswahl, um die Rentabilität zu steigern. Selbst wenn das Ziel nicht in der Generierung von Umsatz besteht – z. B. bei nationalstaatlichen Aktivitäten für geopolitische Zwecke –, kommen sowohl zufällige als auch gezielte Angriffe zum Einsatz. Im vergangenen Jahr setzten Internetkriminelle weiterhin auf Social Engineering und die Nutzung aktueller Themen für die Maximierung ihres Erfolgs. Während beispielsweise COVID-bezogene Phishing-Köder seltener verwendet wurden, beobachteten wir die Zunahme von Ködern, die um Spenden für die Bevölkerung der Ukraine baten.

Angreifer passen sich an und finden neue Wege zum Implementieren ihrer Techniken. Dabei werden sie bei Auswahl von Technik und Standort der Infrastruktur für die Durchführung ihrer Kampagnen immer komplexer. Wir haben beobachtet, dass Internetkriminelle immer sparsamer werden und Angreifer nicht mehr für Technologie bezahlen. Zum Senken ihrer Betriebskosten und Vergrößern des legitimen Anstrichs versuchen manche Angereifer verstärkt, Unternehmen zu kompromittieren: für das Hosten ihrer Phishing-Kampagnen, ihrer Schadsoftware oder sogar zum Nutzen der Rechenleistung für das Minen von Kryptowährung.

In diesem Kapitel untersuchen wir auch die Zunahme von Hacktivismus. Dabei handelt es sich um eine Störung, die auf Privatpersonen zurückzuführen ist, um sozialen oder politischen Zielen Nachdruck zu verleihen. Tausende von Menschen auf der ganzen Welt – Expert*innen ebenso wie Neulinge – haben sich seit Februar 2022 für Angriffe mobilisiert. Dazu gehört das Abschalten von Websites und das Durchsickernlassen gestohlener Daten als Teil des Krieges zwischen Russland und der Ukraine. Es ist noch zu früh, um vorherzusehen, ob sich dieser Trend nach dem Ende aktiver Feindseligkeiten fortsetzt.

Organisationen müssen ihre Zugriffskontrollen regelmäßig überprüfen und stärken und Sicherheitsstrategien zur Abwehr von Cyberattacken implementieren. Das ist jedoch nicht alles, was sie tun können. Wir erklären, wie unsere Digital Crimes Unit (DCU) zivile Fälle genutzt hat, um bösartige Infrastrukturen zu beschlagnahmen, die von Cyberkriminellen und nationalstaatlichen Akteuren genutzt wurden. Wir müssen diese Bedrohung gemeinsam durch öffentliche und private Partnerschaften bekämpfen. Wir hoffen, dass wir anderen durch die Weitergabe unserer Erfahrungen aus den letzten zehn Jahren dabei helfen werden, die proaktiven Maßnahmen zu verstehen und zu berücksichtigen, die sie ergreifen können, um sich selbst und die breiter gefasste Infrastruktur vor der kontinuierlich ansteigenden Bedrohung durch Cyberkriminalität zu schützen.

Amy Hogan-Burney
General Manager, Digital Crimes Unit

Ransomware und Erpressung: eine Bedrohung auf nationaler Ebene

Ransomware-Angriffe stellen eine immer größere Gefahr für alle dar, weil kritische Infrastruktur, Unternehmen jeder Größe sowie kommunale und Bundesbehörden von Kriminellen angegriffen werden, die auf eine wachsende cyberkriminelle Infrastruktur zurückgreifen können.

In den letzten zwei Jahren haben aufsehenerregende Ransomware-Vorfälle, z. B. in Zusammenhang mit kritischer Infrastruktur, Gesundheitswesen und IT-Dienstleistern, für großes öffentliches Interesse gesorgt. Weil Ransomware-Angriffe mit zunehmender Aggressivität immer weiter um sich greifen, haben auch die Auswirkungen immer weiter reichende Folgen. Im Folgenden finden Sie Beispiele für Angriffe, die wir 2022 bereits erlebt haben:

- Im Februar hat ein Angriff auf zwei Unternehmen die Zahlungsverarbeitungssysteme von Hunderten von Tankstellen in Norddeutschland betroffen.[1]
- Im März hat ein Angriff gegen den griechischen Postdienst die Postzustellung vorübergehend lahmgelegt und die Verarbeitung von Finanztransaktionen beeinträchtigt.[2]
- Ende Mai führte ein Ransomware-Angriff auf Costa Ricas Regierungsbehörden zur Ausrufung eines nationalen Notstands, nachdem Krankenhäuser keine Versorgung mehr bieten konnten und die Einziehung von Zöllen und Steuern gestört wurde.[3]
- Ebenfalls im Mai verursachte ein Angriff Flugverspätungen und Stornierungen bei einer der größten indischen Fluggesellschaften, sodass Hunderte von Passagieren strandeten.[4]

Der Erfolg dieser Angriffe und das Ausmaß ihrer realen Auswirkungen sind das Ergebnis einer Industrialisierung der kriminellen Cyberwirtschaft, die den Zugang zu Tools und Infrastruktur sowie die Ausweitung der cyberkriminellen Fähigkeiten ermöglicht.

In den letzten Jahren hat sich Ransomware verlagert – von einem Modell, bei dem eine einzelne „Bande“ eine Ransomware-Nutzlast entwickelt und bereitstellt, hin zu einem RaaS-Modell (Ransomware-as-a-Service). RaaS ermöglicht einer Gruppe, die Ransomware-Nutzlast zu entwickeln und Dienstleistungen zur Durchführung von Bezahlung und Erpressung über Datenlecks für einen Anteil am Gewinn an andere Cyberkriminelle bereitzustellen – also an diejenigen, die die Ransomware-Angriffe tatsächlich starten. Letztere werden als „Partner“ bezeichnet. Durch dieses Franchising der cyberkriminellen Wirtschaft hat sich der Pool der Angreifer erweitert. Die Industrialisierung von cyberkriminellen Tools hat es Angreifern leichter gemacht, Eindringversuche durchzuführen, Daten zu exfiltrieren und Ransomware bereitzustellen.

Von Menschen platzierte Ransomware[5] (Human-operated Ransomware) bleibt eine erhebliche Bedrohung für Unternehmen. Der Begriff wurde von Microsoft-Forschenden geprägt, um Bedrohungen zu beschreiben, die von Menschen gesteuert werden, die in jeder Phase der Angriffe Entscheidungen treffen. Dabei reagieren sie auf das, was sie im Zielnetzwerk vorfinden, und weichen von vorkonfektionierten Ransomware-Angriffen ab.

Modell basierend auf Daten aus Microsoft Defender for Endpoint (EDR) (Januar–Juni 2022)

Ransomware und Erpressung: eine Bedrohung auf nationaler Ebene

Fortsetzung

Ransomware-Angriffe entfalten inzwischen noch größere Wirkung, weil mittlerweile eine Strategie zur doppelten Monetarisierung der Erpressung gängige Praxis ist. Dabei werden Daten aus kompromittierten Geräten exfiltriert und auf den Geräten verschlüsselt. Danach werden die gestohlenen Daten entweder öffentlich gepostet oder es wird damit gedroht, sie öffentlich zu machen, um die Opfer zur Zahlung eines Lösegelds zu zwingen.

Zwar infizieren die meisten Ransomware-Angreifer opportunistisch jedes Netzwerk, auf das sie Zugriff erlangen, doch manche kaufen den Zugriff auch von anderen Cyberkriminellen und machen sich die Verbindungen zwischen Access Brokern und Betreibern von Ransomware zunutze.

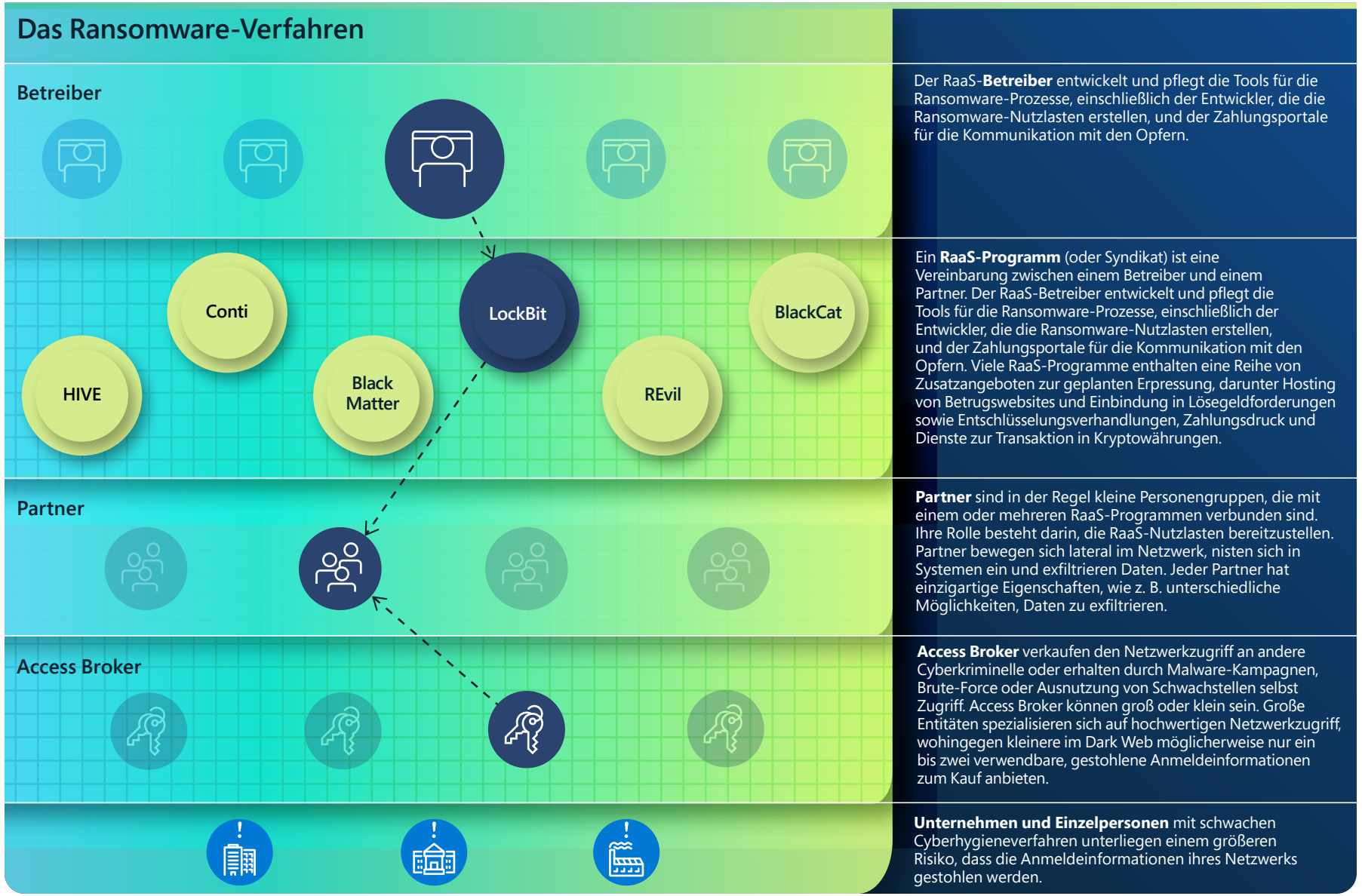
Unsere einzigartige Bandbreite an signalerfassender Aufklärung speist sich aus mehreren Quellen – Identität, E-Mails, Endpunkte und Cloud – und bietet Insights in die wachsende Ransomware-Wirtschaft, die auch ein System von Partnern mit Tools für technisch versierte Angreifer umfasst.

Die Ausweitung der Beziehungen zwischen spezialisierten Cyberkriminellen hat das Tempo, die Raffinesse und den Erfolg von Ransomware-Angriffen erhöht. Daher hat sich die kriminelle Infrastruktur zunehmend in ein Geflecht aus vernetzten Akteuren mit unterschiedlichen Techniken, Zielen und Fähigkeiten entwickelt, die sich gegenseitig beim ersten Zugriff auf Ziele, bei Zahlungsdienstleistungen und bei Entschlüsselungs- oder Veröffentlichungstools oder -Websites unterstützen.

Ransomware-Betreiber können nun online Zugriff auf Organisationen oder Behördennetzwerke erwerben oder Anmeldeinformationen und Zugriff über zwischenmenschliche Beziehungen mit Händlern erhalten, deren Hauptziel ausschließlich darin besteht, den erreichten Zugriff zu monetarisieren.

Die Betreiber nutzen den gekauften Zugriff anschließend zum Bereitstellen einer Ransomware-Nutzlast, die über Marktplätze oder Foren im Darknet erworben wurde. In vielen Fällen werden die Verhandlungen mit den Opfern vom RaaS-Team und nicht von den Betreibern selbst geführt. Diese kriminellen Transaktionen verlaufen reibungslos, und aufgrund der Anonymität im Darknet und der Schwierigkeiten bei der länderübergreifenden Durchsetzung von Gesetzen ist das Risiko einer Verhaftung und Anklage für die Beteiligten gering.

Nachhaltige und erfolgreiche Initiativen gegen diese Bedrohung erfordern eine gesamtstaatliche Strategie in enger Partnerschaft mit dem privaten Sektor.



Im Gegensatz dazu, wie Ransomware manchmal in den Medien dargestellt wird, kommt es eher selten vor, dass eine einzelne Variante von Ransomware von einer autarken „Ransomware-Bande" gesteuert wird. Stattdessen gibt es separate Entitäten, die Malware entwickeln, Zugriffsdaten von Opfern erbeuten, Ransomware bereitstellen und Erpressungsverhandlungen führen. Die Industrialisierung der kriminellen Infrastruktur führte zu Folgendem:

- Access Broker, die in Systeme einbrechen und den Zugriff weitergeben (Access-as-a-Service)
- Entwickler von Schadsoftware, die Tools verkaufen
- Kriminelle Betreiber und Partner, die Eindringversuche durchführen
- Verschlüsselungs- und Erpressungsdienstleister, die die Monetarisierung von Partnern (RaaS) übernehmen

Alle Kampagnen mit von Menschen platzierter Ransomware hängen von den gleichen Sicherheitsschwächen ab. In der Regel profitieren Angreifer insbesondere von schlechter Cyberhygiene eines Unternehmens. Dazu gehört häufig seltenes Patchen und das Versäumnis, Multi-Faktor-Authentifizierung (MFA) zu implementieren.

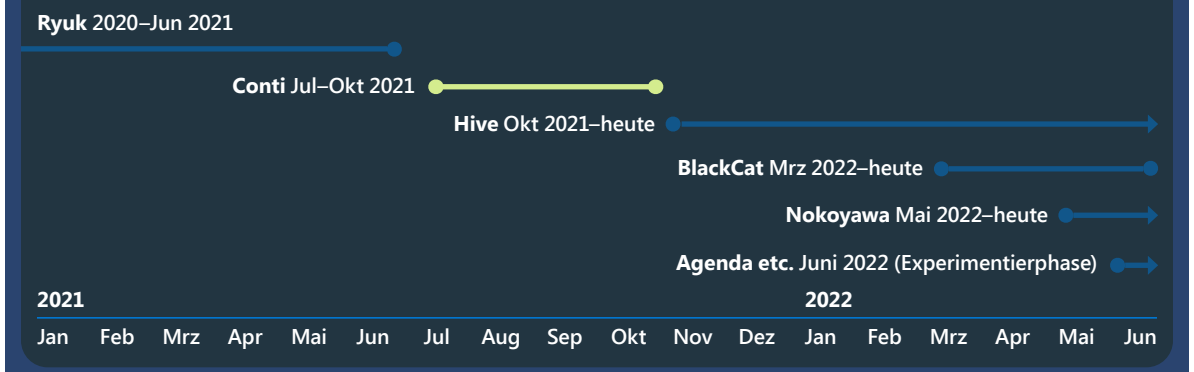
Fallstudie: Die Zerschlagung von Conti

Conti, eine der wichtigsten Ransomware-Varianten der letzten zwei Jahre, stellte ab Mitte 2022 den Betrieb nach und nach ein. Das Microsoft Threat Intelligence Center (MSTIC) beobachtete Ende März und Anfang April einen deutlichen Rückgang der Aktivitäten. Die letzten Bereitstellungen von Conti-Ransomware verzeichneten wir Mitte April. Wie schon das Stilllegen anderer Ransomware-Operationen hatte auch die Liquidierung von Conti allerdings keine nennenswerten Auswirkungen auf die Bereitstellung von Ransomware an sich. Das MSTIC stellte fest, dass Conti-Partner stattdessen auf andere Ransomware-Nutzlasten wie BlackBasta, Lockbit 2.0, LockbitBlack und HIVE umschwenkten. Dies deckt sich mit den Daten aus den Vorjahren und impliziert, dass Ransomware-Banden, wenn sie offline gegangen sind, einige Monate später wieder auftauchen oder ihre technischen Fähigkeiten und Ressourcen neuen Gruppen zur Verfügung stellen.

Unsere Microsoft Threat Intelligence-Teams verfolgen Ransomware-Akteure als einzelne Gruppen (genannt DEVs) anhand ihrer spezifischen Tools, und nicht anhand der von ihnen verwendeten Schadsoftware. Dadurch konnten wir nach der Zerschlagung von Conti die entsprechenden DEVs über die Verwendung von Tools oder RaaS-Kits weiterhin verfolgen. Zum Beispiel:

- DEV-0230, der/die mit Trickbot in Zusammenhang steht, war ein/e produktive/r Benutzer*in von Conti. Ende April beobachtete MSTIC DEV-0230 bei der Nutzung von QuantumLocker.
- DEV-0237 verlagerte sich von Contis Ransomware-Kit zu HIVE und Nokoyawa, einschließlich des Einsatzes von HIVE beim Angriff vom 31. Mai auf Regierungsbehörden von Costa Rica.
- DEV-0506, ein/e weitere/r sehr aktive/r Benutzer*in des Conti Ransomware Kits, wurde mit BlackBasta beobachtet.

Beispiel eines Partners (DEV-0237), der schnell zwischen RaaS-Programmen wechselt



Nachdem ein RaaS-Programm wie Conti abgeschaltet wurde, wechselt der Ransomware-Partner fast sofort zu einem anderen (Hive).

RaaS befeuert die Entwicklung der Ransomware-Infrastruktur und erschwert Zuschreibungen

Da von Menschen platzierte Ransomware von einzelnen Betreibern gesteuert wird, variieren die Angriffsmuster je nach Ziel und ändern sich ständig während eines laufenden Angriffs. In der Vergangenheit haben wir in jeder Kampagne eines einzelnen Ransomware-Stamms eine enge Beziehung zwischen den getroffenen Entscheidungen in Bezug auf den ersten Einfallsvektor, die Tools und die Ransomware-Nutzlast beobachtet. Dies hat die Zuschreibung erleichtert. Dieses Beziehungsgeflecht wird jedoch durch das RaaS-Partnermodell entkoppelt. Infolgedessen verfolgt Microsoft nun Ransomware-Partner, die Nutzlasten bei spezifischen Angriffen bereitstellen, anstatt der Entwickler der Ransomware-Nutzlast als Betreiber.

Anders ausgedrückt: Wir gehen nicht mehr davon aus dass die HIVE-Entwickler auch die Betreiber hinter einem Angriff mit HIVE-Ransomware sind. Wahrscheinlich ist es eher ein Partner.

Die Cybersicherheitsbranche hat bisher Schwierigkeiten, diese Trennung zwischen Entwicklern und Betreibern angemessen zu erfassen. Die Branche meldet Ransomware-Vorfälle nach wie vor anhand des Namens der jeweiligen Nutzlast. Das erweckt den falschen Eindruck, dass eine einzelne Entität – oder Ransomware-Bande – hinter sämtlichen Angriffen steht, die mit dieser bestimmten Ransomware-Nutzlast durchgeführt werden, und dass alle damit verbundenen Vorfälle auf dieselben Techniken und dieselbe Infrastruktur zurückgreifen. Zur Unterstützung der Verteidiger von Netzwerken muss unbedingt mehr über die Phasen in Erfahrung gebracht werden, die den verschiedenen Angriffen durch Partner vorausgehen, z. B. Exfiltration von Daten und zusätzliche Persistenzmechanismen, sowie über die vorhandenen Möglichkeiten für Aufspürung und Schutz.

Mehr noch als Schadsoftware benötigen Angreifer Anmeldeinformationen, um ihre Prozesse erfolgreich durchführen zu können. Die erfolgreiche Infektion eines ganzen Unternehmens mit von Menschen platzierter Ransomware hängt vom Zugriff auf ein Konto mit hohen Berechtigungen ab.

Schlaglicht auf von Menschen platzierte Ransomware-Angriffe

Im vergangenen Jahr haben die Ransomware-Expert*innen von Microsoft gründliche Untersuchungen zu mehr als 100 von Menschen platzierten Ransomware-Vorfällen durchgeführt, um die Techniken von Angreifern nachzuverfolgen und zu verstehen, wie unsere Kund*innen besser geschützt werden können.

Bitte beachten Sie, dass die hier präsentierte Analyse nur für integrierte, verwaltete Geräte möglich ist. Nicht integrierte, unverwaltete Geräte sind der unsicherste Teil der Hardwareressourcen eines Unternehmens.

Am weitesten verbreitete Techniken der Ransomware-Phase:

75 %

Nutzung von Admin-Tools.

75 %

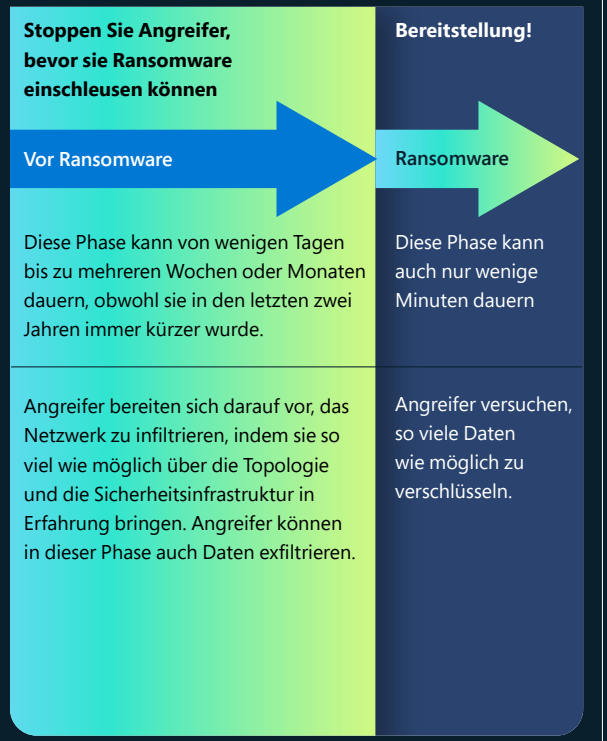
Nutzung von gekaperten höherwertigen kompromittierten Benutzerkonten zur Verbreitung bösartiger Nutzlasten über das SMB-Protokoll

99 %

Manipulationsversuche mit gefundenen Sicherheits-und Sicherungsprodukten mithilfe betriebssystembasierter Tools

Der übliche Ablauf eines von Menschen platzierten Angriffs

Von Menschen platzierte Ransomware-Angriffe können in die Vor-Ransomware-Phase und die Ransomware-Bereitstellungsphase eingeordnet werden. Während der Vor-Ransomware-Phase bereiten sich Angreifer darauf vor, das Netzwerk zu infiltrieren, indem sie die Typologie und Sicherheitsinfrastruktur des Unternehmens ausforschen.



Unsere Untersuchungen zeigten, dass die meisten Akteure hinter von Menschen platzierten Ransomware-Angriffen ähnliche Sicherheitsschwächen nutzen und Gemeinsamkeiten bei Angriffsmustern und -techniken aufweisen.

Eine robuste Sicherheitsstrategie

Die Bekämpfung und Abwehr von Angriffen dieser Art verlangt von Organisationen eine neue Denkweise, sodass sie sich auf den lückenlosen Schutz konzentrieren, der erforderlich ist, um Angreifer zu verlangsamen und aufzuhalten, bevor sie von der Vor-Ransomware-Phase in die Ransomware-Bereitstellungsphase übergehen können.

Um Angriffe zu verhindern, müssen Unternehmen bewährte Sicherheitsmethoden konsistent und aggressiv auf ihre Netzwerke anwenden. Weil die Entscheidungen von Menschen getroffen werden, können diese Ransomware-Angriffe mehrere, scheinbar unterschiedliche Warnmeldungen von Sicherheitsprodukten auslösen, die möglicherweise entweder übersehen werden oder auf die nicht rechtzeitig reagiert werden kann. Alarmmüdigkeit ist eine Tatsache, und Sicherheitsteams in SOCs (Security Operations Centers) können sich das Leben erleichtern, indem sie Trends in ihren Warnmeldungen betrachten oder Warnungen in Vorfälle gruppieren, damit sie das größere Bild sehen können. SOCs können Warnungen mithilfe von Hardening-Funktionen vermindern, z. B. durch Regeln zur Reduzierung der Angriffsfläche. Das Hardening gegen häufige Bedrohungen kann nicht nur die Menge der Warnmeldungen verringern, sondern auch viele Angreifer stoppen, noch bevor es ihnen gelingt, Zugriff auf Netzwerke zu erlangen.

Organisationen müssen kontinuierlich hohe Sicherheitsstandards und Netzwerkhygiene aufrechterhalten, um sich vor von Menschen platzierten Ransomware-Angriffen zu schützen.

Umsetzbare Insights

Ransomware-Angreifer*innen haben es auf schnelles und leicht zu verdienendes Geld abgesehen. Bei der Bekämpfung dieser Art von Cyberkriminalität ist es daher entscheidend, die Kosten, die den Tätern entstehen, durch bessere Sicherheitsmechanismen nach oben zu treiben.

1. Achten Sie auf Hygiene bei Ihren Zugangsdaten. Mehr noch als Schadsoftware benötigen Angreifer Anmeldeinformationen, um ihre Prozesse erfolgreich durchführen zu können. Die erfolgreiche Infektion eines ganzen Unternehmens mit von Menschen platzierter Ransomware hängt vom Zugriff auf ein Konto mit hohen Berechtigungen ab, z. B. ein Domänenadministrator oder Berechtigungen zum Bearbeiten einer Gruppenrichtlinie.
2. Überwachen Sie die Offenlegung von Zugangsdaten.
3. Priorisieren Sie die Bereitstellung von Active Directory-Updates.
4. Priorisieren Sie das Hardening der Cloud.
5. Verringern Sie die Angriffsfläche.
6. Stärken Sie die Sicherheit für mit dem Internet verbundene Ressourcen, und erfassen Sie Ihren Perimeter vollständig.
7. Wirken Sie der Alarmmüdigkeit von SOCs mit Netzwerk-Hardening entgegen, um die Anzahl von Warnmeldungen zu reduzieren und Bandbreite für Vorfälle mit hoher Priorität freizuhalten.

Links zu weiteren Informationen

- RaaS: Understanding the cybercrime gig economy and how to protect yourself | Microsoft Security Blog
- Human-operated ransomware attacks: A preventable disaster | Microsoft Security Blog

Ransomware-Insights von Front-Respondern

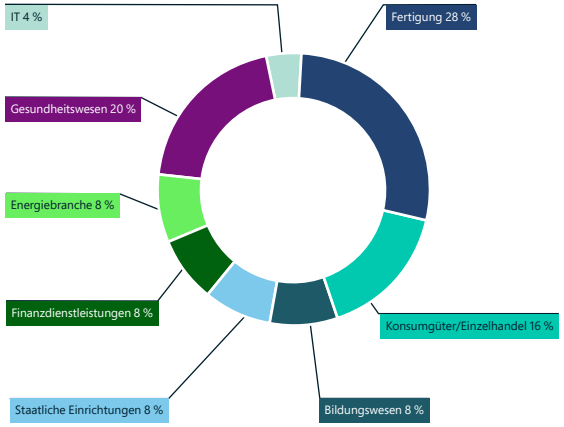
Seit 2019 erleben Unternehmen weltweit ein stetiges Wachstum bei von Menschen platzierten Ransomware-Angriffen. Allerdings hatten Strafverfolgungsmaßnahmen und geopolitische Ereignisse im letzten Jahr erhebliche Auswirkungen auf kriminelle Organisationen.

Die Security Service Line von Microsoft unterstützt Kund*innen während aller Phasen eines Cyberangriffs – von der Untersuchung bis hin zu erfolgreichen Eindämmungs- und Wiederherstellungsaktivitäten. Die Reaktions- und Wiederherstellungsservices werden über zwei eng verzahnte Teams angeboten. Ein Team konzentriert sich auf die Untersuchung und die Schaffung der Grundlagen für die Wiederherstellung, das andere auf Eindämmung und Wiederherstellung. Dieser Abschnitt enthält eine Zusammenfassung der Ergebnisse, die auf Ransomware-Vorfällen im letzten Jahr basieren.

93 %

der von Microsoft durchgeführten Untersuchungen während der Wiederherstellung nach Ransomware-Angriffen zeigten unzureichende Kontrollen über Berechtigungszugriff und laterale Bewegungen.

Ransomware-Vorfälle und Wiederherstellungen nach Branche

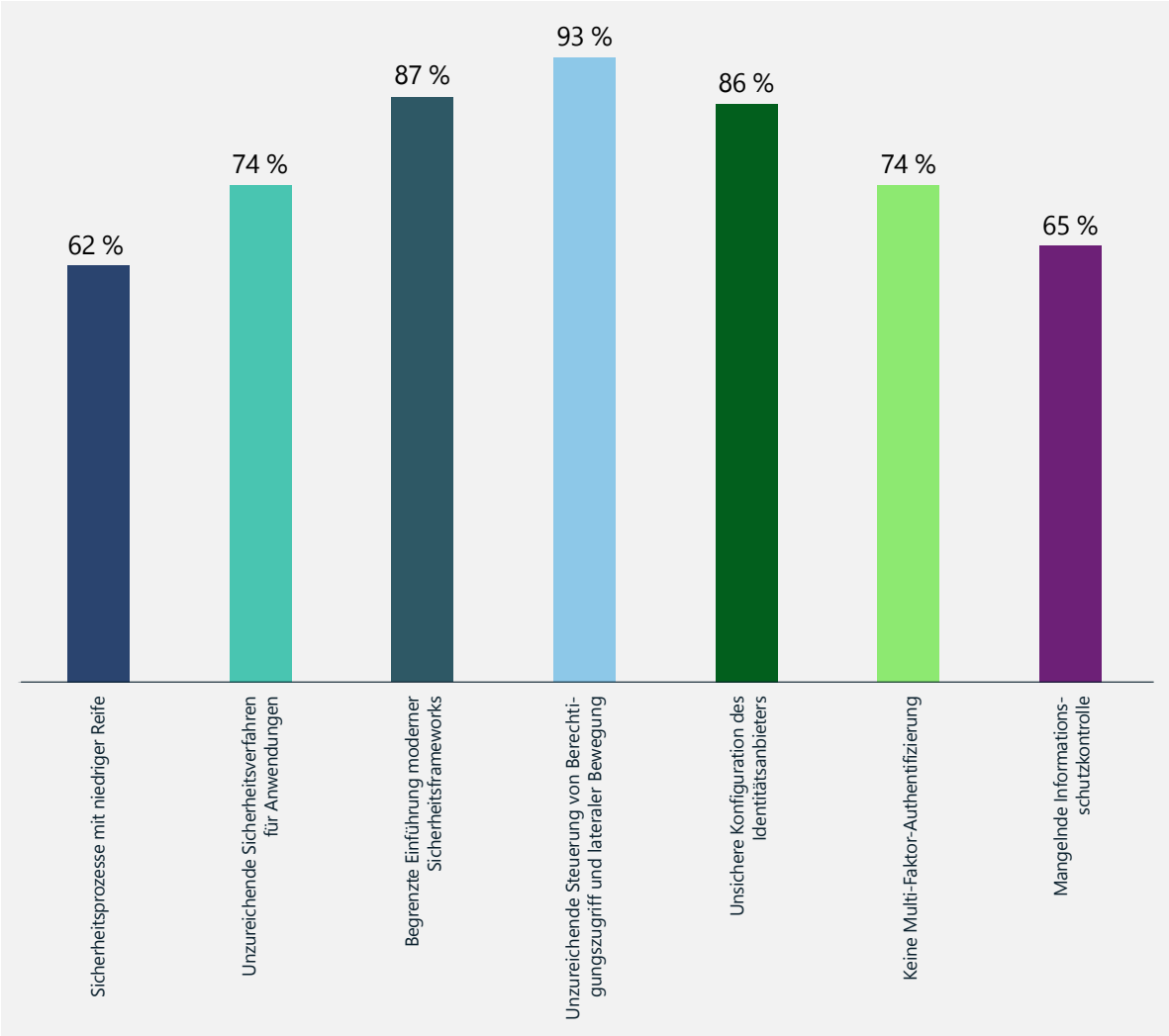


Wenn neue kleine Gruppen und Bedrohungen die Bühne betreten, müssen die Verteidigungsteams die aufkommenden Ransomware-Bedrohungen kennen und gleichzeitig gegen zuvor unbekannte Familien von Ransomware-Schadsoftware gewappnet sein. Der Ansatz der schnellen Entwicklung, den kriminelle Gruppen verfolgen, zog die Entwicklung intelligenter Ransomware nach sich, die in benutzungsfreundlichen Kits verpackt ist. Dies ermöglicht eine größere Flexibilität beim Starten umfassender Angriffe auf eine höhere Anzahl von Zielen.

Auf den folgenden Seiten sehen Sie die am häufigsten beobachteten Faktoren, die zu einem schwachen Schutz vor Ransomware führen. Die Befunde sind in drei Kategorien unterteilt:

1. Schwache Identitätskontrollen
2. Ineffektive Sicherheitsmaßnahmen
3. Eingeschränkter Datenschutz

Zusammenfassung der häufigsten Befunde bei der Reaktion auf Ransomware



Die häufigsten Befunde bei der Reaktion auf Ransomware-Vorfälle waren unzureichende Kontrollen über den Berechtigungszugriff und laterale Bewegungen.

Ransomware-Insights von Front-Respondern

Fortsetzung

Die drei wichtigsten Faktoren, die bei unseren Reaktionseinsätzen vor Ort aufgetreten sind:

① **Schwache Identitätskontrollen:** Diebstahl von Anmeldeinformationen bleibt einer der wichtigsten Faktoren

② **Ineffektive Sicherheitsmaßnahmen** bieten Angreifern nicht nur ein Einfallstor, sondern haben auch erhebliche Auswirkungen auf die benötigte Zeit für eine Wiederherstellung.

③ Letztendlich läuft alles auf die Daten hinaus: Unternehmen haben Probleme mit der Implementierung einer effektiven **Datenschutzstrategie**, die sich an ihren geschäftlichen Anforderungen orientiert.

① Schwache Identitätskontrollen

Von Menschen platzierte Ransomware entwickelt sich weiter und verwendet Diebstahl von Anmeldeinformationen sowie Methoden lateraler Bewegung, die herkömmlicherweise mit gezielten Angriffen einhergehen. Erfolgreiche Angriffe sind oft das Ergebnis langfristiger Kampagnen, bei denen Identitätssysteme wie Active Directory (AD) kompromittiert werden, die den menschlichen Betreibern den Diebstahl von Anmeldeinformationen, den Zugriff auf Systeme und den persistenten Verbleib im Netzwerk ermöglichen.

Active Directory (AD) und Azure AD-Sicherheitsfunktionen

88 %

der betroffenen Kund*innen haben keine bewährten Methoden für AD- und Azure AD-Sicherheitsfunktionen verwendet. Dies hat sich zu einem häufigen Angriffsvektor entwickelt, weil Angreifer fehlerhafte Konfigurationen und schwächere Sicherheitsstatus in kritischen Identitätssystemen ausnutzen, um einen ausgeweiteten Zugriff auf Unternehmen zu erhalten und größere Wirkung zu erzielen.

Zugriff mit den geringstmöglichen Berechtigungen und Nutzung von Privileged Access Workstations (PAW)

Keines der betroffenen Unternehmen hatte bei der Verwaltung seiner kritischen Identitätsressourcen und anderer hochwertiger Ressourcen, wie proprietärer Systeme und geschäftskritischer Anwendungen, eine ordnungsgemäße Trennung von Admin-Anmeldeinformationen und Prinzipien des Zugriffs mit den geringstmöglichen Berechtigungen implementiert.

Sicherheit privilegierter Konten

88 %

der Vorfälle: MFA war nicht für sensitive Konten und Konten mit hohen Privilegien implementiert. Dies hinterließ eine Sicherheitslücke, über die Angreifer Anmeldeinformationen kompromittieren und mit legitimen Anmeldeinformationen weitere Angriffe durchführen konnten.

84 %

Administratoren in 84 % der Unternehmen nutzten keine Kontrollen der Berechtigungsidentität, z. B. Just-in-Time-Zugriff, um eine weitere böswillige Verwendung kompromittierter privilegierter Anmeldeinformationen zu verhindern.

Ransomware-Insights von Front-Respondern

Fortsetzung

② Ineffektive Sicherheitsmaßnahmen

Unsere Daten zeigen, dass Unternehmen, die Ransomware-Angriffe erlitten haben, erhebliche Lücken bei ihren Sicherheitsmaßnahmen und Tools sowie bei der Lebenszyklusverwaltung ihrer IT-Ressourcen aufweisen. Anhand der verfügbaren Daten wurden die folgenden Lücken am häufigsten beobachtet:

Patchen:

68 %

der betroffenen Organisationen besaßen keinen effektiven Prozess zur Verwaltung von Sicherheitsrisiken und Patches, und eine hohe Abhängigkeit von manuellen Prozessen – im Gegensatz zum automatischen Patchen – führte zu kritischen Einfallstoren. Die Fertigungsbranche und Betreiber kritischer Infrastrukturen haben weiterhin Probleme mit der Wartung und dem Patchen von älteren OT-Systemen (Operational Technology).

Fehlende Tools für die Sicherheitsmaßnahmen:

Die meisten Unternehmen meldeten einen Mangel an durchgängiger Sicherheitstransparenz aufgrund fehlender oder fehlerhafter Konfigurationen von Sicherheitstools, was zu einer geringeren Effektivität bei Erkennung und Reaktion führte.

60 %

der Organisationen meldeten, dass kein EDR[6]-Tool verwendet wurde – eine grundlegende Technologie für Erkennung und Reaktion.

60 %

tätigten keine Investitionen in SIEM-Technologie (Security Information and Event Management). Dies führte zu Silobildungen bei der Überwachung, eingeschränkten Fähigkeiten bei der Erkennung durchgängiger Bedrohungen sowie zu ineffizienten Sicherheitsmaßnahmen. Automatisierung ist nach wie vor eine entscheidende Lücke bei SOC-Tools und -Prozessen und zwingt SOC-Mitarbeiter dazu, unzählige Stunden mit dem Interpretieren von Sicherheitstelemetrie zu verbringen.

84 %

der betroffenen Organisationen ermöglichten keine Integration ihrer Multi-Cloud-Umgebungen in ihre Sicherheitstools.

Reaktions- und Wiederherstellungsprozesse:

76 %

Das Fehlen eines effektiven Reaktionsplans war ein kritischer Bereich, der in 76 % der betroffenen Organisationen beobachtet wurde. Dies verhinderte eine angemessene Krisenvorbereitung und wirkte sich negativ auf die erforderliche Zeit für Reaktion und Wiederherstellung aus.

③ Eingeschränkter Datenschutz

Vielen kompromittierten Unternehmen fehlten ordnungsgemäße Datenschutzprozesse, was erhebliche Auswirkungen auf die Wiederherstellungszeiten und die Fähigkeit zur Rückkehr zum regulären Geschäftsbetrieb hatte. Zu den häufigsten Lücken zählen:

Unveränderliche Sicherung:

44 %

der Organisationen besitzen keine unveränderlichen Sicherungen für die betroffenen Systeme. Daten zeigen auch, dass Administratoren keine Sicherungen und Wiederherstellungspläne für kritische Ressourcen wie AD haben.

Data Loss Prevention:

Angreifern gelingt die Kompromittierung von Systemen in der Regel durch die Ausnutzung von Schwachstellen von Organisationen, indem sie kritische Daten exfiltrieren, um sie für Erpressung, den Diebstahl geistigen Eigentums oder zur Monetarisierung zu nutzen.

92 %

der betroffenen Organisationen implementierten keine effektiven Kontrollen für Data Loss Prevention, um die entsprechenden Risiken abzuschwächen, was zu kritischem Datenverlust führte.

Das Aufkommen von Ransomware ist in einigen Regionen gesunken und in anderen gestiegen.

In diesem Jahr haben wir einen Rückgang der Gesamtzahl von Ransomware-Fällen beobachtet, die unseren Reaktionsteams in Nordamerika und Europa im Vergleich zum Vorjahr gemeldet wurden. Gleichzeitig stiegen die gemeldeten Fälle in Lateinamerika.

Auch wenn die Strafverfolgungsaktivitäten die Angriffshäufigkeit in Jahre 2022 wahrscheinlich gesenkt hat, könnten die Akteure durchaus neue Strategien entwickeln, um einer Entlarvung in Zukunft zu entgehen.

Eine Interpretation dieser Beobachtung sind Cyberkriminelle, die sich von Bereichen, die ihrer Wahrnehmung nach ein höheres Risiko einer Strafverfolgung haben, zugunsten weicherer Ziele abgewendet haben. Da Microsoft keine wesentliche Verbesserung bei der weltweiten Sicherheit von Unternehmensnetzwerken beobachtete, die eine Abnahme der mit Ransomware zusammenhängenden Supportanrufe erklären würde, gehen wir davon aus, dass die wahrscheinlichste Ursache in einer Kombination aus Strafverfolgungsaktivitäten in den Jahren 2021 und 2022 liegt, die die Kosten krimineller Aktivitäten in die Höhe getrieben haben. Auch einige geopolitische Ereignisse des Jahres 2022 spielten eine Rolle.

Einer der am weitesten verbreiteten RaaS-Prozesse gehört zu einer russischsprachigen kriminellen Gruppe namens REvil (auch bekannt als Sodinokibi), die seit 2019 aktiv ist. Im Oktober 2021 wurden die Server von REvil im Rahmen der internationalen Polizeiaktion „GoldDust“ abgeschaltet.[7] Im Januar 2022 verhaftete Russland 14 angebliche REvil-Mitglieder und führte Razzien an 25 Standorten durch, die mit ihnen in Verbindung standen.[8] Dies war das erste Mal, dass Russland auf eigenem Boden gegen Ransomware-Betreiber vorging.

2 x

Ransomware-Angriffe sind in einigen Regionen gesunken, aber die Lösegeldforderungen haben sich mehr als verdoppelt.

Auch wenn die Strafverfolgungsaktivitäten die Angriffshäufigkeit in Jahre 2022 wahrscheinlich gesenkt hat, könnten die Akteure durchaus neue Strategien entwickeln, um einer Entlarvung in Zukunft zu entgehen. Darüber hinaus scheinen die Spannungen zwischen Russland und den USA aufgrund des russischen Angriffskriegs gegen die Ukraine die noch in den Kinderschuhen steckende Kooperation Russlands im globalen Kampf gegen Ransomware ein Ende gesetzt zu haben. Nach einer kurzen Zeit der Unsicherheit im Nachgang der REvil-Verhaftungen haben die USA und Russland ihre Zusammenarbeit bei der Verfolgung von Ransomware-Akteuren eingestellt. Das bedeutet, dass Cyberkriminelle Russland wieder als sicheren Hafen betrachten könnten.

Mit Blick auf die Zukunft prognostizieren wir, dass das Tempo der Ransomware-Aktivitäten von einigen wichtigen Fragen abhängt:

1. Werden Regierungen Maßnahmen ergreifen, um Ransomware-Kriminelle daran zu hindern, innerhalb ihrer Grenzen zu operieren, oder sich bemühen, Akteure an Aktivitäten im Ausland zu hindern?
2. Werden Ransomware-Gruppen ihre Taktik ändern, um die Notwendigkeit von Ransomware zu beseitigen und stattdessen auf direkte Erpressung bei ihren Angriffen setzen?
3. Werden Organisationen es schaffen, ihre IT-Prozesse schneller zu modernisieren und zu transformieren, als Kriminelle Schwachstellen ausnutzen können?
4. Werden Fortschritte bei der Nachverfolgung und Aufspürung von Lösegeldzahlungen die Empfänger zwingen, Taktiken und Verhandlungsmethoden zu ändern?

Umsetzbare Insights

1. Konzentrieren Sie sich auf ganzheitliche Sicherheitsstrategien, da alle Ransomware-Familien die gleichen Sicherheitsschwächen ausnutzen, um ein Netzwerk zu beeinflussen.
2. Aktualisieren und pflegen Sie Sicherheitsgrundlagen, um den Tiefenschutz bei der Verteidigung zu stärken und die Sicherheitsmaßnahmen zu modernisieren. Ein Umstieg auf die Cloud ermöglicht Ihnen, Bedrohungen schneller zu entdecken und zügiger zu reagieren.

Links zu weiteren Informationen

- Protect your organization from ransomware | Microsoft Security
- 7 ways to harden your environment against compromise | Microsoft Security Blog
- Improving AI-based defenses to disrupt human-operated ransomware | Microsoft 365 Defender Research Team
- Security Insider: Explore the latest cybersecurity insights and updates | Microsoft Security

Cyberverbrechen als Dienstleistung

Cybercrime-as-a-Service (CaaS) ist eine wachsende und sich entwickelnde Bedrohung für Kund*innen auf der ganzen Welt. Die Microsoft Digital Crimes Unit (DCU) hat das kontinuierliche Wachstum der CaaS-Infrastruktur beobachtet. Sie umfasst eine wachsende Anzahl von Onlinediensten, die verschiedene Cyberverbrechen ermöglichen, darunter BEC und von Menschen platzierte Ransomware. Phishing ist nach wie vor eine bevorzugte Angriffsmethode, da Cyberkriminelle erheblich von einem erfolgreichen Diebstahl und Verkauf des Zugriffs auf gestohlene Accounts profitieren.

Als Reaktion auf den expandierenden CaaS-Markt hat die DCU ihre Listening-Systeme verbessert, um CaaS-Angebote in der gesamten Infrastruktur des Internets, im Deep Web, in geprüften Foren,[9] auf dedizierten Websites, in Onlinediskussionsforen und auf Messaging-Plattformen zu erkennen und zu identifizieren.

Cyberkriminelle arbeiten jetzt über Zeitzonen und Sprachen hinweg, um spezifische Ergebnisse zu liefern. So kann eine CaaS-Website, die von einer Person in Asien verwaltet wird, beispielsweise in Europa betrieben werden und bösartige Konten in Afrika erstellen. Die multijurisdiktionale Natur dieser Operationen stellt die Strafverfolgungsbehörden vor komplexe Herausforderungen. Als Reaktion darauf konzentriert sich die DCU auf die Deaktivierung bösartiger krimineller Infrastrukturen, die für CaaS-Angriffe eingesetzt werden, und arbeitet weltweit mit Strafverfolgungsbehörden zusammen, um Kriminelle zur Verantwortung zu ziehen.

Internetkriminelle nutzen zunehmend Analytics, um die Reichweite, den Umfang und den Gewinn zu maximieren. Genau wie legitime Unternehmen müssen CaaS-Websites die Authentizität ihrer Produkte und Dienstleistungen sicherstellen, um einen guten Ruf aufrechtzuerhalten. Beispielsweise automatisieren CaaS-Websites routinemäßig den Zugriff auf kompromittierte Konten, um sicherzustellen, dass die gestohlenen Anmeldeinformationen gültig sind. Sobald die Kennwörter zurückgesetzt oder Schwachstellen gepatcht wurden, stellen die Cyberkriminellen den Verkauf der entsprechenden Konten ein. Wir haben eine zunehmende Menge von CaaS-Websites identifiziert, die Käufer*innen als Teil ihrer Qualitätskontrolle auf Anfrage mit Verifizierungen versorgen. Auf diese Weise können die Käufer*innen sicher sein, dass die CaaS-Website aktive Konten und Kennwörter verkauft. Gleichzeitig senkt es die potenziellen Kosten, die den CaaS-Händlern entstehen, wenn die gestohlenen Anmeldeinformationen vor dem Verkauf geändert und die Schwachstellen beseitigt werden.

Die DCU beobachtete auch CaaS-Websites, die Käufer*innen die Möglichkeit bieten, kompromittierte Konten aus bestimmten geografischen Standorten, von bestimmten Onlinedienstleistern und gezielt von bestimmten Einzelpersonen, Berufsgruppen und Branchen zu erwerben. Bei häufig bestellten Konten geht es vor allem um Fachkräfte oder Abteilungen, die sich mit Rechnungsstellung befassen, z. B. CFOs oder „Debitoren". Auch Branchen, die an öffentlichen Verträgen beteiligt sind, werden aufgrund der Datenmengen, die bei öffentlichen Ausschreibungen verfügbar werden, häufig zum Ziel.

Die DCU-Untersuchungen von CaaS haben eine Reihe von wichtigen Trends aufgezeigt:

Die Anzahl und Komplexität der Services steigt.

Ein Beispiel ist die Entwicklung von Web-Shells. Sie bestehen in der Regel aus kompromittierten Webservern, die zur Automatisierung von Phishing-Angriffen genutzt werden. Die DCU beobachtete, wie CaaS-Händler das Hochladen von Phishing-Kits oder Schadsoftware durch spezialisierte Web-Dashboards vereinfachten. Häufig versuchen CaaS-Verkäufer anschließend, den Bedrohungsakteuren über das Dashboard weitere Services zu verkaufen, z. B. Dienstleistungen in Bezug auf Spam-Nachrichten und spezielle Empfängerlisten für Spam anhand definierter Attribute wie geografischer Standort oder Beruf. In einigen Fällen haben wir festgestellt, dass eine einzelne Web-Shell für mehrere Angriffskampagnen verwendet wurde. Dies legt nahe, dass die Akteure möglicherweise einen dauerhaften Zugriff auf den kompromittierten Server aufrechterhalten. Wir haben auch einen Anstieg der in der CaaS-Infrastruktur verfügbaren Anonymisierungsdienste verzeichnet sowie Angebote für VPN- und VPS-Konten. In den meisten Fällen wurden die angebotenen VPN/VPS zunächst über gestohlene Kreditkarten beschafft. CaaS-Websites boten auch eine größere Anzahl von Zugängen zu Remote-Desktop-Protokoll (RDP), Secure Shell (SSH) und cPanels an, um diese als Plattform zur Orchestrierung von kriminellen Cyberangriffen zu verwenden. CaaS-Händler konfigurieren RDP, SSH und cPanels mit entsprechenden Tools und Skripten, um verschiedene Arten von Cyberattacken zu ermöglichen.

Für Dienstleistungen zur Erstellung von Homoglyphen-Domänen sind zunehmend Zahlungen in Kryptowährungen erforderlich.

Homoglyphen-Domänen geben sich als rechtmäßige Domänennamen aus. Dabei verwenden sie Zeichen, die mit anderen Zeichen identisch sind oder ihrem Erscheinungsbild nahekommen. Das Ziel besteht darin, den Betrachter*innen vorzugaukeln, dass es sich bei der Homoglyphen-Domäne um die echte handelt. Diese Domänen sind eine allgegenwärtige Bedrohung und ein Einfallstor für eine beträchtliche Menge von cyberkriminellen Aktivitäten. CaaS-Websites verkaufen jetzt benutzerdefinierte Homoglyphen-Domänennamen. Die Käufer*innen können also bestimmte Firmen- und Domänennamen anfordern, deren Identität sie nachahmen möchten. Nach Eingang der Zahlung verwenden die CaaS-Händler ein bestimmtes Tool, einen Homoglyphen-Generator, um den Domänennamen auszuwählen und anschließend den bösartigen Homoglyphen zu registrieren. Die Bezahlung dieser Dienstleistung erfolgt fast ausschließlich in Kryptowährung.

2.750.000

Seitenregistrierungen wurden von der DCU in diesem Jahr erfolgreich blockiert, um kriminellen Akteuren zuvorzukommen, die sie für weltweite Cyberkriminalität einsetzen wollten.

Cyberverbrechen als Dienstleistung

Fortsetzung

CaaS-Verkäufer bieten in zunehmendem Maße kompromittierte Anmeldeinformationen zum Kauf an.

Kompromittierte Anmeldeinformationen ermöglichen den unbefugten Zugriff auf Benutzerkonten, einschließlich E-Mail-Nachrichtendiensten, Ressourcen für die gemeinsame Nutzung von Dateien und OneDrive for Business. Wenn die Administratoranmeldeinformationen kompromittiert wurden, können unbefugte Benutzer auf vertrauliche Dateien, Azure-Ressourcen und unternehmenseigene Benutzerkonten zugreifen. In vielen Fällen zeigten die DCU-Untersuchungen, dass dieselben unbefugten Anmeldeinformationen gleich auf mehreren Servern verwendet wurden, um deren Verifizierung zu automatisieren. Dieses Muster legt nahe, dass die kompromittierten Benutzer*innen möglicherweise mehreren Phishing-Angriffen zum Opfer fallen oder von einer bösartigen Gerätesoftware befallen sind, die Botnet-Keyloggern das Abfischen von Anmeldeinformationen ermöglicht.

CaaS-Dienste und -Produkte mit erweiterten Funktionen zum Vermeiden einer Entdeckung greifen immer weiter um sich.

Ein CaaS-Verkäufer bietet für gerade mal 6 USD pro Tag Phishing-Kits mit noch mehr Komplexitätstiefe und Anonymisierungsfunktionen an, die darauf ausgelegt sind, Erkennungs- und Präventionssysteme zu umgehen. Die Dienstleistung umfasst eine Reihe von Umleitungen, die Prüfungen durchführen, bevor der Datenverkehr zur nächsten Ebene oder Website zugelassen wird. Eine davon führt mehr als 90 Prüfungen durch, um einen Fingerabdruck des Geräts zu erstellen. Dazu gehört festzustellen, ob es sich um eine virtuelle Maschine handelt, das Sammeln von Daten über den verwendeten Browser und die verwendete Hardware und vieles mehr. Wenn alle Prüfungen erfolgreich sind, wird der Datenverkehr an eine für das Phishing verwendete Zielseite gesendet.

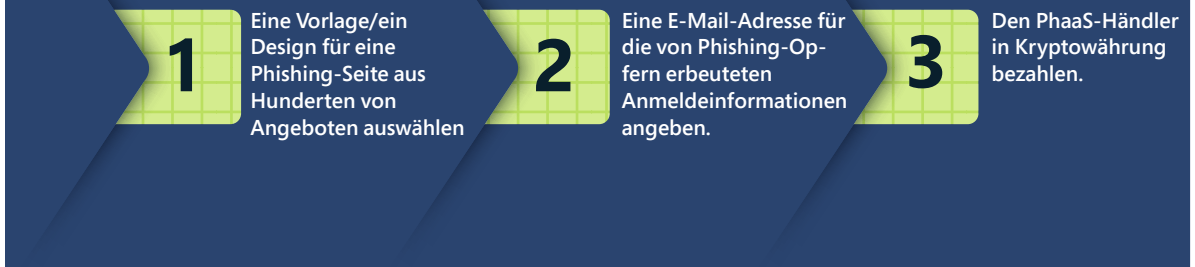
Durchgängige Cybercrime-Dienste verkaufen Abonnements von Managed Services.

In der Regel kann jeder Schritt bei der Anbahnung eines Onlineverbrechens die Akteure entlarven, wenn die operative Sicherheit zu gering ist. Das Risiko von Offenlegung und Identifizierung steigt, wenn Dienste von mehreren CaaS-Sites erworben werden. Die DCU beobachtete einen Trend im Darknet: Das Angebot an Dienstleistungen zum Anonymisieren von Softwarecode und Generisieren von Websitetexten, um das Risiko einer Aufdeckung zu reduzieren, wird größer. Anbieter von durchgängigen Abonnementdiensten für Cyberkriminalität verwalten alle Dienste und garantieren Ergebnisse, die das Risiko einer Offenlegung für den abonnierenden OCN weiter senken. Das reduzierte Risiko hat die Beliebtheit dieser durchgängigen Dienstleistungen gesteigert.

Phishing-as-a-Service (PhaaS) ist ein Beispiel für einen durchgängigen Cybercrime-Dienst. PhaaS ist eine Weiterentwicklung eines früheren Service namens FUD (Fully Undetectable Services) und wird in Form eines Abonnements angeboten. Zu den üblichen Nutzungsbedingungen von PhaaS gehört es, Phishing-Websites einen Monat aktiv zu lassen.

Die DCU hat auch einen CaaS-Händler identifiziert, der Distributed Denial of Service (DDoS) als Abonnementmodell anbietet. Bei diesem Modell wird die Erstellung und Pflege des für die Durchführung der Angriffe erforderlichen Botnets an den CaaS-Händler ausgelagert. Alle DDoS-Abonnementkund*innen erhalten einen verschlüsselten Dienst, um die operative Sicherheit zu erhöhen, sowie ein Jahr lang Support rund um die Uhr. Der DDoS-Abonnementdienst bietet verschiedene Architekturen und Angriffsmethoden. Die Käufer*innen wählen also einfach eine Ressource, die sie angreifen möchten, und der Händler stellt Zugriff auf eine Reihe von kompromittierten Geräten auf seinem Botnet bereit, um den Angriff durchzuführen. Die Kosten für das DDoS-Abonnement liegen bei nur 500 USD.

PhaaS: Cyberkriminelle bieten mehrere Dienstleistungen in einem einzigen Abonnement an. Die Käufer*innen müssen in der Regel nur drei Dinge tun:



Sobald diese Schritte abgeschlossen sind, erstellt der PhaaS-Händler Dienste mit drei oder vier Umleitungsebenen sowie Hostingressourcen für den gezielten Angriff auf bestimmte Benutzende. Die Kampagne wird anschließend gestartet, und die Anmeldeinformationen der Opfer werden abgerufen, überprüft und an die vom Käufer angegebene E-Mail-Adresse gesendet. Für eine Prämie bieten viele PhaaS-Händler an, Phishing-Sites auf der öffentlichen Blockchain zu hosten, sodass sie von jedem Browser abgerufen werden können und die Umleitungen Benutzende auf eine Ressource im Distributed Ledger verweisen können.

Die Arbeit der DCU zur Entwicklung von Tools und Techniken, die CaaS-Internetkriminelle identifizieren und unterbrechen, wird laufend fortgesetzt. Durch die Weiterentwicklung von CaaS-Diensten entstehen erhebliche Herausforderungen, insbesondere bei der Störung von Zahlungen in Kryptowährung.

Kriminelle Nutzung von Kryptowährungen

Kryptowährungen sind mittlerweile auch im Mainstream angekommen. Entsprechend greifen Kriminelle immer mehr auf sie zurück, um einer Strafverfolgung zu entgehen und Maßnahmen zur Bekämpfung von Geldwäsche zu umgehen. Dies erhöht die Herausforderung für Strafverfolgungsbehörden, Zahlungen in Kryptowährung an Internetkriminelle aufzuspüren und nachzuverfolgen.

Die weltweiten Ausgaben für Blockchainlösungen stiegen in den letzten vier Jahren um rund 340 %, während die Anzahl neuer Wallets für Kryptowährungen um rund 270 % wuchs. Es gibt mehr als 83 Millionen einzigartige Wallets weltweit, und die gesamte Marktkapitalisierung aller Kryptowährungen lag am 28. Juli 2022 bei etwa 1,1 Billionen USD.[10]

Quelle: Twitter.com – @PeckShieldAlert (PeckShield ist ein in China ansässiges Unternehmen für Blockchainsicherheit).

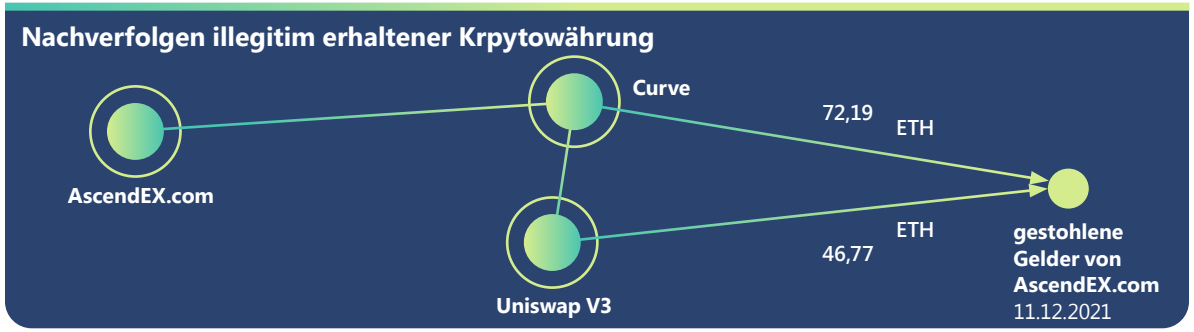
Nachverfolgen von Ransomware-Zahlungen

Ransomware ist eine der größten Quellen von illegal erbeuteter Kryptowährung. In dem Bemühen, die bösartige technische Infrastruktur, die bei Ransomware-Angriffen eingesetzt wird, zu zerstören – wie z. B. bei der Zerschlagung von Zloander im April 2022[11] – spürt die DCU von Microsoft kriminelle Wallets auf, um das Nachverfolgen und Wiederherstellen von Kryptowährungen zu ermöglichen.

DCU-Forschende haben beobachtet, dass Ransomware-Akteure ihre Taktik bei der Kommunikation mit Opfern weiterentwickeln, um die Spur des Geldes zu verwischen. Ursprünglich gaben die Cyberkriminellen in ihren Lösegeldforderungen Bitcoin-Adressen an. Dies machte die Verfolgung des Zahlungsverkehrs zur Blockchain jedoch leicht. Daher hörten Ransomware-Akteure damit auf, Wallet-Adressen anzugeben, und fügten stattdessen E-Mail-Adressen oder Links zu Chatwebseiten hinzu, um den Opfern dort die Adressen für die Zahlung des Lösegelds mitzuteilen. Manche Akteure erstellten sogar für jedes Opfer eine eigene Webseite mit einem eigenen Login. Auf diese Weise wollten sie Sicherheitsforschende und Strafverfolgungsbehörden daran hindern, die Wallet-Adressen der Kriminellen zu erhalten, indem sie vorgaben, selbst Opfer zu sein. Trotz aller Bemühungen der Kriminellen, ihre Spuren zu verwischen, können einige Lösegeldzahlungen dank der Zusammenarbeit mit Strafverfolgungsbehörden und Krypto-Analytics-Unternehmen, die Bewegungen auf der Blockchain analysieren, immer noch nachverfolgt werden.

Trend: DEX-Wäsche von illegalen Erträgen

Ein zentrales Problem für Cyberkriminelle ist der Umtausch von Kryptowährung in Fiatwährung. Cyberkriminelle können beim Umtausch zwischen mehreren Optionen wählen. Jede davon ist in unterschiedlichem Maße riskant. Eine Methode zur Risikoreduzierung besteht darin, den Erlös über einen dezentralen Umtausch (Decentralized Exchange, DEX) zu waschen, bevor er über verfügbare Auszahlungsoptionen, wie z. B. zentralisierten Umtausch (Centralized Exchange, CEX), Peer-to-Peer (P2P) und Over-the-Counter (OTC) ausbezahlt wird. DEXes sind eine attraktive Möglichkeit zur Geldwäsche, da sie häufig keine Maßnahmen zur Bekämpfung von Geldwäsche befolgen.



Mithilfe von Chainalysis, einem investigativen Tool für Kryptowährungen, hat die Digital Crimes Unit von Microsoft AcendEX-Hacker entdeckt, die ihre gestohlenen Gelder neben Uniswap auch noch an einem kleineren DEX namens Curve umtauschten. Dieses Diagramm zeigt die vom Team enthüllten Wege der Geldwäsche. Jeder Kreis steht für einen Cluster von Wallets. Die Zahlen an den einzelnen Linien zeigen den Gesamtbetrag, den Ethereum zum Zwecke der Geldwäsche übermittelt hat.

Im Dezember 2021 griffen Hacker die globale Kryptowährungs-Handelsplattform AscendEx an und stahlen etwa 77, 7 Millionen USD in Kryptowährung an Kundengeldern.[12] AscendEx engagierte daraufhin Blockchain-Analytics-Unternehmen und nahm mit anderen CEXs Kontakt auf, um die Wallets mit den gestohlenen Geldern auf eine Schwarze Liste zu setzen. Darüber hinaus wurden Adressen, an die die Coins gesendet wurden, auf dem Ethereum Blockchain-Explorer Etherscan entsprechend markiert.[13] Um die Warnungen und die Schwarze Liste zu umgehen, schickten die Hacker am 18. Februar 2022 1, 5 Millionen USD in Ethereum an einen der weltweit größten DEXes.[14]

Die Einführung stärkerer Anti-Geldwäschemaßnahmen seitens der DEXes verpasste den Geldwäscheaktivitäten auf ihren Plattformen einen Dämpfer und zwang die Cyberkriminellen, auf andere Verschleierungsmethoden zurückzugreifen, z. B. „Coin Tumbling" oder unlizenzierte Umtauschmöglichkeiten. Beispielsweise kündigte Uniswap vor Kurzem an, dass die Plattform damit beginnen wird, Wallets, die bekanntermaßen an illegitimen Aktivitäten beteiligt sind, über eine Schwarze Liste von Transaktionen auf ihrem Umtauschmarkt auszuschließen.[15]

Umsetzbare Insights

1. Wenn Sie Opfer von Cyberkriminalität geworden sind und die Kriminellen mit Kryptowährung bezahlt haben, nehmen Sie Kontakt zu Ihren örtlichen Strafverfolgungsbehörden auf. Möglicherweise können diese Ihnen helfen, die Gelder zu verfolgen und zurückzuerhalten.
2. Erkundigen Sie sich vor der Auswahl eines DEX nach den jeweils vorhandenen Maßnahmen gegen Geldwäsche.

Links zu weiteren Informationen

- Hardware-based threat defense against increasingly complex cryptojackers | Microsoft 365 Defender Research Team

Die Entwicklung der Phishing-Bedrohungslandschaft

Phishing-Verfahren zur Erbeutung von Anmeldeinformationen nehmen zu und bleiben überall eine erhebliche Bedrohung für Benutzer*innen, da sie wahllos alle Posteingänge ins Visier nehmen. Unter den Bedrohungen, denen unsere Forschenden nachgehen und vor denen sie für Schutz sorgen, ist die Menge an Phishing-Angriffen um mehrere Größenordnungen höher als bei allen anderen Bedrohungen.

Mithilfe von Daten aus Defender for Office können wir Aktivitäten mit böswilligen E-Mails und kompromittierter Identität sehen. Azure Active Directory Identity Protection bietet über Warnmeldungen zu Ereignissen in Zusammenhang mit kompromittierten Identitäten zudem noch weitere Informationen. Über Defender for Cloud Apps erkennen wir Ereignisse des Datenzugriffs mit kompromittierter Identität, und Microsoft 365 Defender (M365D) stellt produktübergreifende Zusammenhänge her. Die Kennzahl zur lateralen Bewegung stammt von Defender for Endpoint (Warnmeldungen und Ereignisse zum Angriffsverhalten), Defender for Office (böswillige E-Mails) und auch hier wieder M365D (für die produktübergreifende Korrelation).

710 Millionen
blockierte Phishing-E-Mails pro Woche

1 Std., 12 Min.
Die durchschnittliche Zeit, die ein Angreifer benötigt, um auf Ihre privaten Daten zuzugreifen, wenn Sie einer Phishing-E-Mail zum Opfer fallen.[16]

1 Std., 42 Min.
Die durchschnittliche Zeit, die ein Angreifer zur Verfügung hat, um damit zu beginnen, sich nach der Kompromittierung eines Geräts in Ihrem Unternehmensnetzwerk lateral zu bewegen.[17]

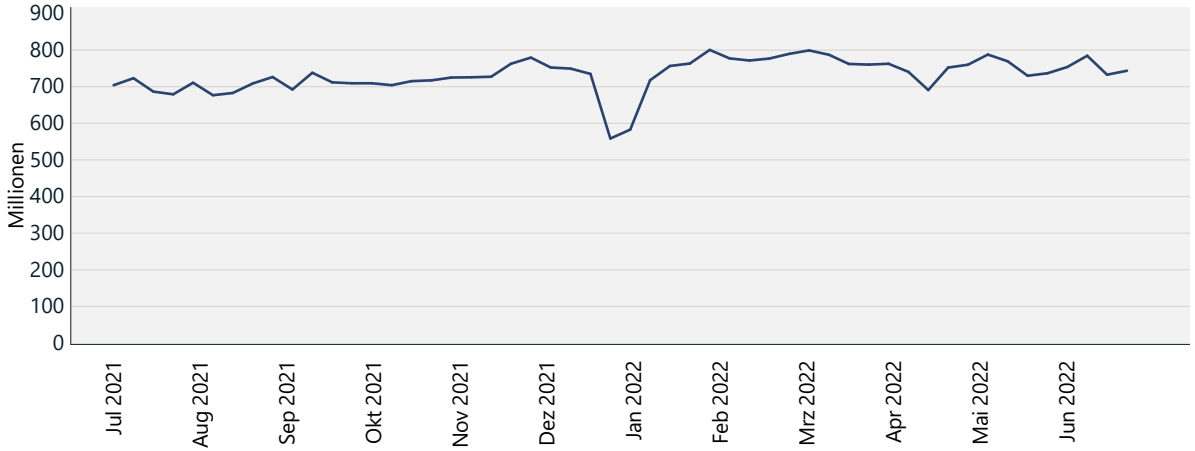
Microsoft 365 zählt beim Erbeuten von Anmeldeinformationen nach wie vor zu den begehrtesten Kontotypen für Angreifer. Sobald die Anmeldeinformationen kompromittiert sind, können sich Angreifer bei zum Unternehmen gehörenden Computersystemen anmelden, um die Infektion mit Schadsoftware und Ransomware durchzuführen, vertrauliche Unternehmensdaten durch den Zugriff auf SharePoint-Dateien zu stehlen und die Verbreitung von Phishing weiterzuführen, indem sie unter anderem böswillige E-Mails über Outlook verschicken.

Neben Kampagnen mit breit gefassten Zielen nehmen Angreifer mit Phishing zum Erbeuten von Anmeldeinformationen, Spenden und personenbezogenen Daten selektiv Unternehmen ins Visier, um größere Auszahlungen zu erzielen. E-Mail-Phishing-Angriffe gegen Unternehmen werden als „BEC-Angriffe“ bezeichnet. Microsoft entdeckt jeden Monat Millionen von BEC-E-Mails, die 0,6 % aller beobachteten Phishing-E-Mails ausmachen. Ein Bericht von IC3[18] im Mai 2022 zeigt einen Aufwärtstrend bei exponierten Verlusten durch BEC-Angriffe.

Die bei Phishing-Angriffen verwendeten Techniken werden immer komplexer. Als Reaktion auf die Gegenmaßnahmen passen sich die Angreifer an und finden neue Wege zum Implementieren ihrer Techniken. Dabei werden sie bei Auswahl von Technik und Standort der Infrastruktur für die Durchführung ihrer Kampagnen immer komplexer. Dies bedeutet, dass Organisationen ihre Strategie für die Implementierung von Sicherheitslösungen regelmäßig neu bewerten müssen, um böswillige E-Mails zu blockieren und die Zugriffskontrolle für einzelne Benutzerkonten zu stärken.

531.000
Zusätzlich zu den URLs, die von Defender for Office blockiert wurden, war unsere Digital Crimes Unit maßgeblich an der Deaktivierung von 531.000 eindeutigen Phishing-URLs außerhalb von Microsoft beteiligt.

Erkannte Phishing-E-Mails



Die Anzahl der pro Woche erkannten Phishing-Angriffe steigt weiter. Der Rückgang im Dezember und Januar ist ein zu erwartender saisonaler Rückgang, der auch schon im letztjährigen Bericht gemeldet wurde. Quelle: Signale aus Exchange Online Protection

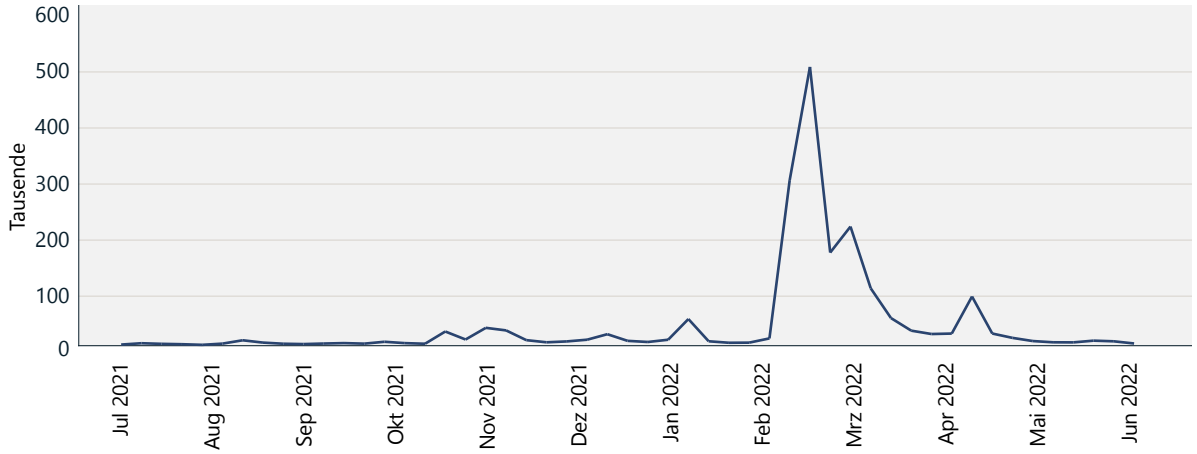
Die Entwicklung der Phishing-Bedrohungslandschaft

Fortsetzung

Wir beobachten weiterhin eine stetige Zunahme von Phishing-E-Mails im Vergleich zum Vorjahr. Der Umstieg auf Remote-Arbeit in den Jahren 2020 und 2021 hat zu einer erheblichen Zunahme von Phishing-Angriffen geführt, die sich den Wandel bei der Arbeitsumgebung zunutze machen wollten. Phishing-Betreiber führen schnell neue E-Mail-Vorlagen ein. Dazu verwenden sie Köder, die sich an großen Weltereignissen orientieren, z. B. an der COVID-19-Pandemie, und an Themen in Zusammenhang mit Tools für Zusammenarbeit und Produktivität wie Google Drive oder OneDrive für Dateifreigaben. Während Themen in Zusammenhang mit COVID-19 abgenommen haben, wurde der Krieg in der Ukraine Anfang März 2022 zu einem neuen Köder. Unsere Forschenden beobachteten eine erstaunliche Zunahme von E-Mails, die vorgaben, von legitimen Organisationen zu stammen und um Spenden in Kryptowährung wie Bitcoin und Ethereum baten, angeblich um ukrainische Bürger zu unterstützen.

Nur wenige Tage nach dem Beginn des Krieges in der Ukraine Ende Februar 2022 stieg die Anzahl der erfassten Phishing-E-Mails mit Ethereum-Adressen bei Unternehmenskunden drastisch an. Die Gesamtzahl der Vorfälle erreichte in der ersten Märzwoche ihren Höhepunkt, als eine halbe Million Phishing-E-Mails die Adresse eines Ethereum-Wallets enthielten. Vor Beginn des Krieges war die Anzahl der Ethereum-Wallet-Adressen in anderen als Phishing erkannten E-Mails deutlich niedriger und lag im Durchschnitt bei einigen Tausend E-Mails pro Tag.

Phishing-E-Mails mit Ethereum-Wallet-Adressen



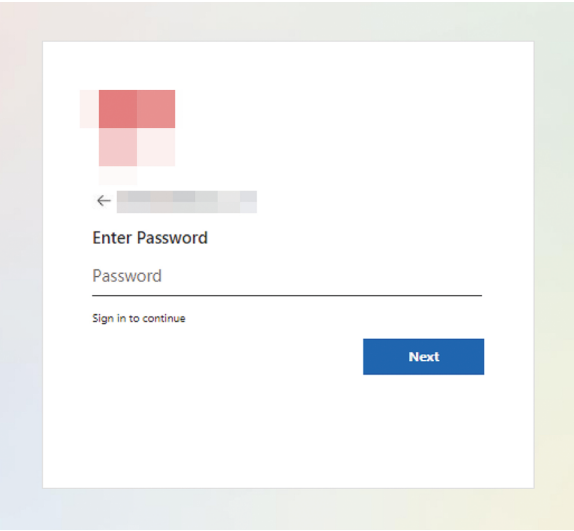
Die Gesamtzahl der E-Mails, die als Phishing mit Ethereum-Wallet-Adressen erkannt wurden, stieg zu Beginn des Konflikts zwischen der Ukraine und Russland steil an und fiel dann wieder ab.

Phisher setzen bei ihren Aktionen mehr denn je auf eine legitime Infrastruktur. Dies führt zu einem Anstieg von Phishing-Kampagnen, die darauf abzielen, verschiedene Aspekte einer Operation zu kompromittieren, sodass sie keine eigene kaufen, hosten oder betreiben müssen. Böswillige E-Mails können beispielsweise von kompromittierten Absenderkonten stammen. Angreifer profitieren von der Verwendung dieser E-Mail-Adressen, die einen höheren Reputationswert genießen und als vertrauenswürdiger angesehen werden als neu erstellte Konten und Domänen. In einigen ausgeklügelteren Phishing-Kampagnen konnten wir beobachten, dass Angreifer ihre Versand- und Spoofing-Aktionen lieber von Domänen mit einer fälschlicherweise als „Keine Aktion"-Richtlinie eingerichteten DMARC-Einstellung[19] ausführen, die E-Mail-Spoofing Tür und Tor öffnen.

Große Phishing-Operationen verwenden in der Regel Cloud-Dienste und virtuelle Cloud-Maschinen (VMs), was Angriffe in großem Maßstab ermöglicht. Angreifer können den von VMs ausgehenden Bereitstellungs- und Auslieferungsvorgänge von E-Mails mithilfe von SMTP-E-Mail-Relais oder cloudbasierter E-Mail-Infrastruktur vollständig automatisieren, um von hohen Auslieferungsraten und dem positiven Ruf dieser legitimen Dienste zu profitieren. Wenn der Versand von böswilligen E-Mails über diese Cloud-Dienste zugelassen wird, müssen sich die Verteidiger auf leistungsstarke E-Mail-Filterfunktionen verlassen, um E-Mails am Eindringen in ihr System zu hindern.

Microsoft-Konten bleiben eines der beliebtesten Ziele für Phishing-Betreiber. Das zeigt sich an den zahlreichen Phishing-Landingpages, die sich als die Microsoft 365-Anmeldeseite ausgeben. Phisher versuchen beispielsweise, die Microsoft-Anmeldeoberfläche in ihren Phishing-Kits zu imitieren, indem sie eine einzigartige URL generieren, die auf den Empfänger abgestimmt ist. Diese URL führt zu einer bösartigen Webseite, die zum Sammeln von Anmeldeinformationen entwickelt wurde. Ein Parameter innerhalb dieser URL enthält jedoch die E-Mail-Adresse des jeweiligen Empfängers. Sobald das Ziel die Seite aufruft, füllt das Phishing-Kit Anmeldedaten der jeweiligen Benutzer*innen automatisch aus und zeigt ein auf den E-Mail-Empfänger abgestimmtes Unternehmenslogo, was die individuelle Microsoft 365-Anmeldeseite des Zielunternehmens imitiert.

Phishing-Seite, die eine Microsoft-Anmeldeseite mit dynamischem Inhalt simuliert

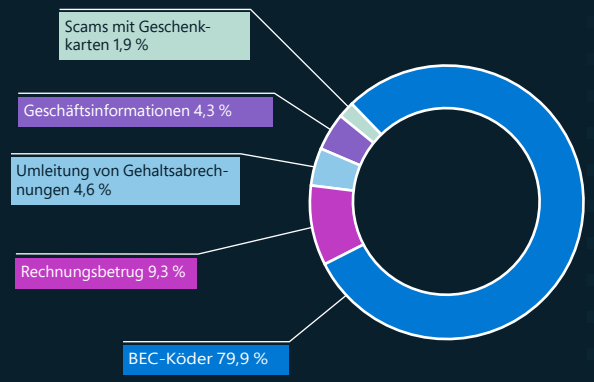


Schlaglicht auf die Kompromittierung geschäftlicher E-Mails

Cyberkriminelle entwickeln immer komplexere Vorgehensweisen und Techniken, um Sicherheitseinstellungen zu überwinden und Einzelpersonen, Unternehmen und Organisationen ins Ziel zu nehmen. Als Reaktion investieren wir erhebliche Ressourcen in die weitere Optimierung unseres BEC-Bekämpfungsprogramms.

Mit schätzungsweise 2,4 Mrd. USD an bereinigten Kosten im Jahre 2021 ist BEC das kostspieligste finanzielle Cyberverbrechen und macht mehr als 59 % der fünf weltweit höchsten Verluste durch Internetkriminalität aus.[20] Um die Größenordnung des Problems zu verstehen und Ansätze für einen optimalen Schutz der Benutzer*innen vor BEC zu finden, haben Forschende von Microsoft die in den Angriffen am häufigsten verwendeten Motive nachvollzogen.

BEC-Themen (Januar–Juni 2022)



Häufigkeit von BEC-Themen in Prozent

BEC-Trends

Als Einstiegspunkt versuchen BEC-Angreifer normalerweise, ein Gespräch mit potenziellen Opfern zu beginnen, um eine Beziehung aufzubauen. Der Angreifer gibt sich als Kollege oder Geschäftsfreund aus und lenkt das Gespräch allmählich in die Richtung eines Geldtransfers. Die Einführungs-E-Mails, die wir als BEC-Köder verfolgen, stellen fast 80 % der erkannten BEC-E-Mails dar. Zu weiteren Trends, die Microsoft-Sicherheitsexpert*innen im letzten Jahr identifiziert haben, gehören:

- Die am häufigsten verwendeten Techniken bei BEC-Angriffen, die 2022 beobachtet wurden, waren Spoofing[21] und die Vortäuschung einer anderen Identität.[22]
- Der BEC-Untertyp, der den größten finanziellen Schaden für die Opfer verursachte, war Rechnungsbetrug (basierend auf dem Volumen und den angeforderten Dollarbeträgen, die bei unseren Ermittlungen zu BEC-Kampagnen zutage traten).
- Diebstahl von Geschäftsdaten, z. B. Kreditorenberichte und Kundenkontakte, ermöglicht den Angreifern, Betrug mit überzeugend wirkenden Rechnungen durchzuführen.
- Die meisten Anfragen zur Umleitung von Gehaltsabrechnungen kamen von kostenlosen E-Mail-Diensten und selten von kompromittierten Konten. Das E-Mail-Volumen aus diesen Quellen zeigte um den Ersten und um den Fünfzehnten eines Monats Ausschläge, also zu den gängigsten Zahlungsterminen.
- Obwohl sie eigentlich als Betrugsmaschen bekannt sind, machten Scams mit Geschenkkarten nur 1,9 % der erkannten BEC-Angriffe aus.

Umsetzbare Insights

Phishing abwehren

Um die Anfälligkeit Ihres Unternehmens gegenüber Phishing zu reduzieren, sollten IT-Administrator*innen die folgenden Richtlinien und Funktionen implementieren:

1. Zwingende Verwendung von MFA für alle Konten, um unbefugten Zugriff zu beschränken
2. Aktivierung von Funktionen für bedingten Zugriff bei Konten mit hohen Berechtigungen, um den Zugriff aus Ländern, Regionen und von IPs zu blockieren, die in der Regel keinen Datenverkehr in Ihrem Unternehmen erzeugen
3. Erwägung der Verwendung physischer Sicherheitsschlüssel für Führungskräfte, an Zahlungs- oder Kaufaktivitäten beteiligte Mitarbeiter*innen und andere privilegierte Konten
4. Zwingende Nutzung von Browsern, die Dienste wie Microsoft SmartScreen unterstützen, um URLs auf verdächtige Verhaltensweisen zu analysieren und den Zugriff auf bekannte bösartige Websites zu blockieren[23]
5. Verwendung einer auf Machine Learning basierenden Sicherheitslösung, die wahrscheinliches Phishing isoliert und URLs sowie Anhänge in eine Sandbox weiterleitet, bevor die E-Mail den Posteingang erreicht. Ein Beispiel für so eine Lösung ist Microsoft Defender for Office 365.[24]
6. Aktivierung von Schutzmaßnahmen gegen Identitätsvortäuschung und Spoofing in Ihrer gesamten Organisation.
7. Konfigurieren von DKIM (DomainKeys Identified Mail)- und DMARC (Domain-based Message Authentication Reporting & Conformance)-Aktionsrichtlinien, um die Zustellung nicht authentifizierter E-Mails zu verhindern, die vorgeben, von seriösen Absendern zu stammen
8. Prüfung von mandanten- und benutzerseitig erstellten Zulassungsregeln und Ausschluss von breitgefächerten domänen- und IP-basierten Ausnahmen. Diese Regeln haben häufig Vorrang und können bekannte böswillige E-Mails durch E-Mail-Filterung zulassen.
9. Regelmäßige Ausführung von Phishing-Simulatoren, um das potenzielle Risiko in Ihrem ganzen Unternehmen zu erheben und anfällige Benutzer*innen zu identifizieren und zu schulen

Links zu weiteren Informationen

- From cookie theft to BEC: Attackers use AiTM phishing sites as entry point to further financial fraud | Microsoft 365 Defender Research Team, Microsoft Threat Intelligence Center (MSTIC)

Täuschung mit Homoglyphen

BEC und Phishing sind gängige Social Engineering-Taktiken. Social Engineering spielt bei Verbrechen eine wichtige Rolle, indem es ein Ziel durch das Erzeugen von Vertrauen davon überzeugt, mit den Kriminellen zu interagieren.

Im herkömmlichen Handel dienen Marken dazu, das Vertrauen in die Herkunft eines Produkts oder Dienstleistung sicherzustellen. Gefälschte Produkte sind Markenmissbrauch. In ähnlicher Weise geben Cyberkriminelle bei einem Phishing-Angriff vor, ein Kontakt zu sein, den das Ziel kennt. Dazu verwenden sie Homoglyphen, um potenzielle Opfer in die Irre zu führen.

Bei einem Homoglyph handelt es sich um einen Domänennamen, der bei BEC für die E-Mail-Kommunikation verwendet wird. Dabei wird ein Zeichen durch ein anderes ersetzt, das mit dem ursprünglichen Erscheinungsbild identisch oder fast identisch ist, um das Ziel zu täuschen.

Homoglyphen-Techniken bei BEC-Versuchen

BEC besteht in der Regel aus zwei Phasen. Die erste umfasst die Kompromittierung von Anmeldedaten. Bei dieser Art der Offenlegung von Anmeldeinformationen kann es sich um das Ergebnis von Phishing-Angriffen oder um Datenschutzverletzungen größeren Ausmaßes handeln. Anschließend werden die Anmeldeinformationen im Darknet verkauft oder gegen etwas anderes eingetauscht.

Die zweite Phase ist die Betrugsphase. In ihr setzen Angreifer die kompromittierten Anmeldeinformationen ein, um mittels E-Mail-Domänen mit Homoglyphen ausgeklügeltes Social Engineering auszuüben.

Verlauf eines BEC-Angriffs

Methode	% der Domänen, mit dieser Homoglyphen-Methode
l anstatt I	25 %
i anstatt l	12 %
q anstatt g	7 %
rn anstatt m	6 %
.cam anstatt .com	6 %
0 anstatt o	5 %
ll anstatt l	3 %
ii anstatt i	2 %
vv anstatt w	2 %
l anstatt ll	2 %
e anstatt a	2 %
nn anstatt m	1 %
ll anstatt I, l anstatt i	1 %
o anstatt u	1 %

Analyse von über 1.700 Homoglyphen-Domänen von Januar bis Juli 2022. Obwohl 170 Homoglyphen-Techniken verwendet wurden, kamen bei 75 % der Domänen nur 14 davon zum Einsatz.

Ein Homoglyph in Aktion

Eine Homoglyphen-Domäne, die mit dem Erscheinungsbild einer dem Opfer bekannten E-Mail-Domäne identisch ist, wird bei einem E-Mail-Anbieter mit einem identischen Benutzernamen registriert. Anschließend wird eine gekaperte E-Mail von der erbeuteten Domäne mit neuen Zahlungsanweisungen gesendet.

Durch die Nutzung von Open-Source-Intelligence und Zugriff auf E-Mail-Threads identifizieren die Kriminellen Personen, die für die Fakturierung und die Zahlungen verantwortlich sind. Anschließend erstellen sie eine E-Mail-Adresse, die auf den ersten Blick von der Person zu kommen scheint, die normalerweise die Rechnungen verschickt. Dieser falsche Identität besteht aus einem identischen Benutzernamen und einer E-Mail-Domäne, die ein Homoglyph des echten Absenders ist.

Die Angreifer kopieren eine E-Mail-Kette mit einer legitimen Rechnung und ändern die Rechnung dann so, dass sie die eigenen Bankdaten enthält. Diese neue, geänderte Rechnung wird dann über die Homoglyphen-E-Mail-Adresse mit der falschen Identität an das Ziel gesendet. Weil der Kontext zu stimmen scheint und die E-Mail echt aussieht, folgt das Ziel häufig den betrügerischen Anweisungen.

Umsetzbare Insights

1. Erzwingen Sie die Nutzung von Browsern, die Dienste wie Safe Links und SmartScreen unterstützen, um URLs auf verdächtige Verhaltensweisen zu analysieren und den Zugriff auf bekannte bösartige Websites zu blockieren.[25]
2. Verwenden Sie eine auf Machine Learning basierende Sicherheitslösung, die wahrscheinliches Phishing isoliert und URLs sowie Anhänge in eine Sandbox weiterleitet, bevor die E-Mail den Posteingang erreicht.

Links zu weiteren Informationen

- Internet Crime Complaint Center (IC3) | Business Email Compromise: The $43 Billion Scam
- Insights zur Spoofintelligenz – Office 365 | Microsoft-Dokumentation
- Insights zum Identitätswechsel – Office 365 | Microsoft-Dokumentation

Eine Zeitleiste der Botnet-Bekämpfung aus der Frühphase der Zusammenarbeit mit Microsoft

Seit mehr als einem Jahrzehnt arbeitet die DCU daran, die Cyberkriminalität proaktiv zu unterbinden, was zu 26 Zerschlagungen von Schadsoftware und nationalstaatlichen Aktionen führte. Weil das DCU-Team modernste Taktiken und Tools einsetzt, um die illegalen Aktivitäten zu unterbinden, entwickeln auch die Cyberkriminellen ihre Herangehensweisen weiter, um die Nase vorn zu behalten. Hier präsentieren wir eine Zeitleiste mit einem Auszug der von der DCU zerschlagenen Botnets sowie der Strategien, die Microsoft anwendete, um sie auszuschalten.

2008

Conficker-Botnet

Beschreibung: Ein sich schnell ausbreitendes Virus, das das Windows-Betriebssystem angreift und Millionen von Computern und Geräten in einem gemeinsamen Netzwerk infizierte und auf der ganzen Welt Netzwerkausfälle verursachte.

Zusammenarbeit: Bildung der Conficker-Arbeitsgruppe, dem ersten Konsortium seiner Art. Um den Bot zu besiegen, ist Microsoft Partnerschaften mit 16 Organisationen auf der ganzen Welt eingegangen.

Reaktion von Microsoft: Die Gruppe hat über viele Gerichtsbarkeiten hinweg zusammengearbeitet und Conficker erfolgreich zur Strecke gebracht.

2009

Waledac-Botnet

Beschreibung: Ein komplexes Spam-Botnet mit US-Domänen, das E-Mail-Adressen sammelte und Spam verteilte, mit dem weltweit bis zu 90.000 Computer infiziert wurden.[26]

Zusammenarbeit: Gründung eines weiteren Konsortiums, des Microsoft Malware Protection Centers (MMPC), das eine enge Zusammenarbeit mit Akademiker*innen zum Schwerpunkt hat.[27]

Reaktion von Microsoft: Microsoft verwendete einen stufenweisen C2-Ansatz und überraschte böswillige Akteure mit der Beschlagnahme von US-Domänen ohne Vorwarnung.[28] Microsoft wurde der vorübergehende Besitz von 280 Domänen zugesprochen, die von den Servern von Waledac verwendet wurden.

2011

Die Microsoft Digital Crimes Unit (DCU) wird gegründet

Zusammenarbeit: Ausgelegt auf das Bekämpfen von Cyberkriminaltät, die sich auf die Microsoft-Infrastruktur auswirkt, durch eine enge Integration eines Teams aus Ermittler*innen, Anwält*innen und Ingenieur*innen.

Herangehensweise von Microsoft: Das Ziel besteht in einem besseren Verständnis der technischen Aspekte verschiedener Schadsoftware und in der Weitergabe dieser Insights an die Rechtsabteilung von Microsoft, um eine effektive Strategie für die Zerschlagung zu entwickeln.

Rustock-Botnet

Beschreibung: Ein Spam-E-Mail-Bot mit einem Backdoor-Trojaner. Hat Internetanbieter als primäre C2s verwendet; für den Verkauf von Arzneimitteln entwickelt.

Zusammenarbeit: Microsoft hat eine Partnerschaft mit Pfizer Pharmaceuticals gegründet, um die von Rustock verkauften Medikamente zu verstehen, und arbeitete eng mit den niederländischen Strafverfolgungsbehörden zusammen.[29]

Reaktion von Microsoft: Microsoft hat eng mit US-Marshalls und Strafverfolgungsbehörden in den Niederlanden zusammengearbeitet, um die C2-Server in dem Land abzuschalten. Alle zukünftigen Domain-Generator-Algorithmen (DGAs) wurden registriert und blockiert.

2013

Sirefef/Zero Access Botnet

Beschreibung: Ein Botnet, das Werbung verbreitete, um die Menschen auf gefährliche Websites zu leiten, die Schadsoftware installierten oder personenbezogene Informationen stahlen. Das Botnet infizierte mehr als zwei Millionen Computer und kostete Werbetreibende mehr als 2,7 Millionen USD pro Monat, vor allem in den USA und Westeuropa.

Zusammenarbeit: Wir arbeiteten eng mit dem FBI und dem Cybercrime Center von Europol zusammen, um die Peer-to-Peer-Infrastruktur zu Fall zu bringen.

Reaktion von Microsoft: Wir wurden Mitglied des Zero-Access-Netzwerks, ersetzten die kriminellen C2-Server und beschlagnahmten erfolgreich Downloadserverdomänen.

2019

Trickbot-Botnet

Beschreibung: Ein ausgeklügeltes Botnet mit über dem Globus verteilter Infrastruktur, das auf die Finanzbranche abzielte; kompromittierte IoT-Geräte.

Zusammenarbeit: Microsoft hat eine Partnerschaft mit dem Financial Services Information Sharing and Analysis Center (FS-ISAC) geschlossen, um Trickbot auszuschalten.[30]

Reaktion von Microsoft: Die DCU hat ein System entwickelt, das Bot-Infrastrukturen identifiziert und nachverfolgt. Das System hat Benachrichtigungen für aktive Internetanbieter generiert, wobei die jeweilige Gesetzgebung in verschiedenen Ländern berücksichtigt wurde.

2022

Kontinuierlicher Fokus auf Zerschlagung

Beschreibung: Im Laufe des letzten Jahres hat Microsoft die Infrastruktur von sieben Akteuren zerschlagen und sie daran gehindert, weitere Schadsoftware in Umlauf zu bringen, die Computer der Opfer zu kontrollieren und noch mehr Opfer anzuvisieren.

Zusammenarbeit: In Partnerschaften mit Internetdienstanbietern, Regierungs- und Strafverfolgungsbehörden sowie mit der Privatwirtschaft gab Microsoft Informationen weiter, um damit weltweit mehr als 17 Millionen Opfern von Schadsoftware zu helfen.

Ein Blick in die Zukunft

Die DCU bleibt Vorreiter und möchte ihre Erfahrung bei der Zerschlagung von Botnets in der Durchführung koordinierter Operationen einbringen, die weit über Schadsoftware hinausgehen. Unser kontinuierlicher Erfolg erfordert kreatives Engineering, den Austausch von Informationen, innovative rechtliche Theorien sowie öffentliche und private Partnerschaften.

Missbrauch von Infrastruktur durch Cyberkriminelle

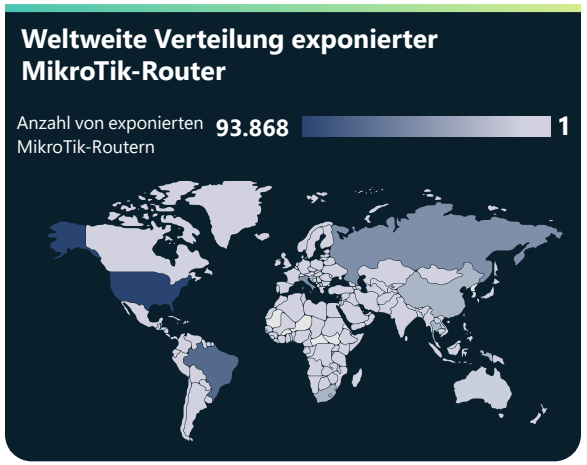
Internetgateways als kriminelle Befehls- und Steuerinfrastruktur

IoT-Geräte werden für Internetkriminelle, die weit verbreitete Botnets nutzen, ein immer beliebteres Ziel. Wenn Router ungepatcht bleiben und direkt dem Internet ausgesetzt sind, können Akteure sie missbrauchen, um auf Netzwerke zuzugreifen, böswillige Angriffe durchzuführen und sogar ihre Operationen zu unterstützen.

Das Team von Microsoft Defender for IoT führt Forschungen zu verschiedenen Arten von Geräten durch, von Legacy-Steuerungen für industrielle Steuerungssysteme bis hin zu hochmodernen IoT-Sensoren. Das Team untersucht IoT- und OT-spezifische Schadsoftware, um einen Beitrag zur gemeinsamen Liste der Anzeichen für Kompromittierung zu leisten.

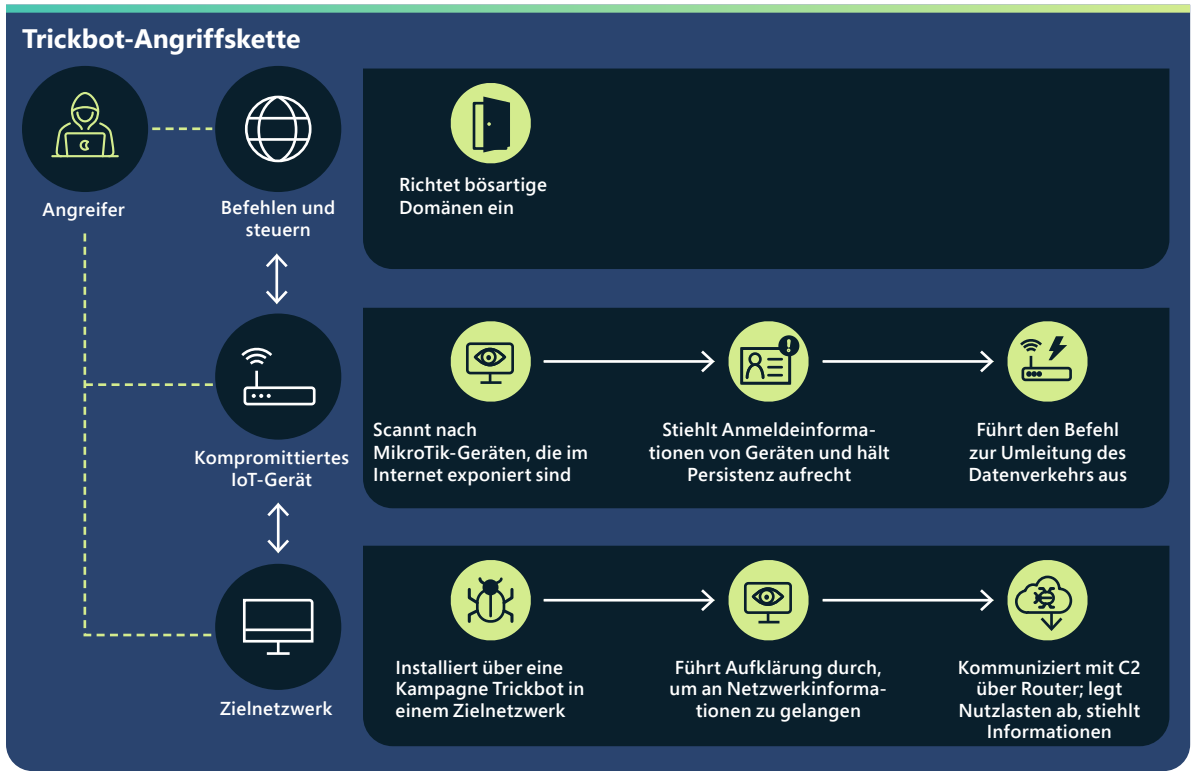
Router sind besonders vulnerable Angriffsvektoren, da sie in Haushalten und Organisationen mit Internetzugang allgegenwärtig sind. Wir verfolgen die Aktivitäten von MikroTik-Routern, ein weltweit beliebter Router in Privathaushalten und Unternehmen, und ermitteln, wie sie zum Befehlen und Steuern (Command and Control, C2), für DNS-Angriffe und zum Kapern von Cryptomining verwendet werden.

Genauer gesagt haben wir ermittelt, wie die Trickbot-Betreiber sich kompromittierte MikroTik-Router zunutze gemacht haben und sie so neu konfigurierten, dass sie als Teil ihrer C2-Infrastruktur agierten. Die Beliebtheit dieser Geräte macht ihren Missbrauch durch Trickbot noch gravierender, und mit ihrer einzigartigen Hardware und Software versetzten sie die Akteure in die Lage, herkömmlichen Sicherheitsmaßnahmen auszuweichen, ihre Infrastruktur auszubauen und noch weitere Geräte und Netzwerke zu kompromittieren.



Für exponierte Router besteht das Risiko, dass potenzielle Schwachstellen ausgenutzt werden.

Durch das Nachverfolgen und Analysieren von Datenverkehr mit SSH-Befehlen (Secure Shell) beobachteten wir, wie Angreifer nach dem Erbeuten legitimer Anmeldeinformationen für Geräte MikroTik-Router für die Kommunikation mit Trickbot-Infrastruktur verwendeten. Diese Anmeldeinformationen können durch Brute-Force-Angriffe abgerufen werden. Dabei werden bekannte Schwachstellen mit leicht verfügbaren Patches ausgenutzt und standardmäßige Kennwörter eingesetzt. Sobald der Zugriff auf ein Gerät gelungen



Trickbot-Angriffskette, die die Verwendung von MikroTik-Geräten als Proxyserver für C2 zeigt.

ist, gibt der Angreifer einen einzigartigen Befehl aus, der den Datenverkehr zwischen zwei Ports zum Router umleitet und die Kommunikationsleitung zwischen von Trickbot betroffenen Geräten und dem C2 etabliert.

Wir haben unser Wissen über die verschiedenen Methoden für Angriffe auf MikroTik-Geräte über Trickbot hinaus sowie über bekannte typische Schwachstellen und Expositionen (Common Vulnerabilities and Exposures, CVEs) in einem Open Source-Tool für MicroTik-Geräte aggregiert. Es kann die forensischen Artefakte in Bezug auf die auf diese Geräte durchgeführten Angriffe extrahieren.[31]

Geräte, die als Reverseproxys für Schadsoftware-C2 fungieren, sind nicht nur bei Trickbot- und MikroTik-Routern eindeutig. In Zusammenarbeit mit dem Microsoft RiskIQ-Team haben wir die beteiligten C2-Server zurückverfolgt und durch die Beobachtung von SSL-Zertifikaten ebenfalls betroffene Ubiquiti- und LigoWave-Geräte identifiziert.[32] Dies ist ein starkes Indiz dafür, dass IoT-Geräte bei koordinierten Angriffen von Nationalstaaten zu aktiven Komponenten und ein beliebtes Ziel für Cyberkriminelle mit weit verbreiteten Botnets werden.

Kryptokriminelle missbrauchen IoT-Geräte

Gateway-Geräte stellen ein zunehmend wertvolles Ziel für Akteure dar, weil die Anzahl bekannter Schwachstellen von Jahr zu Jahr stetig zugenommen hat. Sie werden für Cryptomining und andere Arten von bösartigen Aktivitäten verwendet.

Da Kryptowährungen immer beliebter geworden sind, haben viele Einzelpersonen und Organisationen in Rechenleistung und Netzwerkressourcen von Geräten wie Router investiert, um Coins auf der Blockchain zu minen. Das Minen von Kryptowährung ist jedoch ein zeit- und ressourcenintensiver Prozess mit einer geringen Erfolgswahrscheinlichkeit. Um die Erfolgschancen beim Mining einer Coin zu erhöhen, tun sich Miner in verteilten, kooperativen Netzwerken (Pools) zusammen und erhalten Anteile (Hashes) entsprechend dem prozentualen Anteil an der Coin, den sie mit ihren jeweiligen Ressourcen erfolgreich gemint haben.

Im vergangenen Jahr beobachtete Microsoft eine wachsende Zahl von Angriffen, die Router zur Umleitung von Versuchen des Kryptowährungs-Minings missbrauchen. Cyberkriminelle kompromittieren Router, die mit Mining-Pools verbunden sind, und leiten den Mining-Datenverkehr zu ihren zugehörigen IP-Adressen um. Dies geschieht mittels DNS-Poisoning-Angriffen, bei denen die DNS-Einstellung der angegriffenen Ziele umgeschrieben werden. Betroffene Router registrieren die falsche IP-Adresse für einen bestimmten Domänennamen und senden ihre Mining-Ressourcen – oder Hashes – an Pools, die von Akteuren verwendet werden. Diese Pools könnten anonyme Coins minen, die mit kriminellen Aktivitäten in Verbindung gebracht werden, oder von Minern generierte legitime Hashes verwenden, um einen prozentualen Anteil der von ihnen geminten Coins zu erhalten und damit einen Teil des Gewinns abzuschöpfen.

Da bei mehr als der Hälfte der 2021 bekannten Schwachstellen ein Patch fehlte, bleibt das Aktualisieren und Absichern von Routern in unternehmenseigenen und privaten Netzwerken eine erhebliche Herausforderung für Gerätebesitzer und Administratoren.

Kompromittierung von Geräten für illegales Cryptomining.

Teil der Hashes aus dem ursprünglichen Pool werden von Akteuren gestohlen, oder Ressourcen werden in ihren Pool übertragen, oder Router haben Schadsoftware, die Ressourcen für das Mining stiehlt.

DNS-Poisoning von Gateway-Geräten kompromittiert legitime Miningaktivitäten und leitet Ressourcen zu kriminellen Miningaktivitäten um.

Virtuelle Maschinen als kriminelle Infrastruktur

Der weit verbreitete Umstieg auf die Cloud umfasst auch Cyberkriminelle, die private Ressourcen von ahnungslosen Opfern nutzen. Diese Ressourcen wurden durch Phishing oder die Verbreitung von Schadsoftware, die Anmeldeinformationen abgreift, gestohlen. Viele Cyberkriminelle entscheiden sich dafür, ihre bösartigen Infrastrukturen auf cloudbasierten virtuellen Maschinen (VMs), Containern und Microservices einzurichten.

Sobald die Cyberkriminellen Zugriff erlangt haben, kann es zu einer Ereignisfolge zum Einrichten von Infrastruktur kommen – z. B. eine Reihe von virtuellen Maschinen durch Skripting und automatisierte Prozesse. Diese geskripteten, automatisierten Prozesse werden zum Starten bösartiger Aktivitäten verwendet, z. B. groß angelegte Angriffe mit E-Mail-Spam, Phishing-Angriffe und Webseiten, die verwerfliche Inhalte hosten. Das kann sogar die Einrichtung einer skalierten virtuellen Umgebung umfassen, in der das Mining von Kryptowährungen stattfindet. Das verursacht dem Opfer am Ende des Monats eine Rechnung von mehreren Hunderttausend Dollar.

Die Cyberkriminellen wissen, dass ihre bösartige Aktivität eine begrenze Lebensdauer hat, bevor sie entdeckt und unterbunden wird. Infolgedessen haben sie ihre Bemühungen hochgefahren, agieren jetzt proaktiv und räumen Eventualitäten dabei einen hohen Stellenwert ein. Sie wurden dabei beobachtet, wie sie die kompromittierten Konten weit im Vorwege vorbereiteten und deren Umgebung überwachten. Sobald ein Konto (eingerichtet mithilfe Hunderttausender virtueller Maschinen) enttarnt wird, ziehen sie zum nächsten weiter – das bereits über Skripte vorbereitet wurde und sofort aktiviert werden kann – und setzen ihre bösartigen Aktivitäten mit wenig oder gar keiner Unterbrechung fort.

Wie Cloud-Infrastruktur kann auch On-Premises-Infrastruktur bei Angriffen verwendet werden. Dabei werden lokale Umgebungen verwendet, die den On-Premises-Benutzer*innen unbekannt sind. Dafür muss der ursprüngliche Zugriffspunkt offen und zugänglich bleiben. Auch private On-Premises-Ressourcen wurden von Cyberkriminellen missbraucht, um eine fortschreitende Kette von Cloud-Infrastruktur zu initiieren, die dazu dient, ihren Ursprung zu verschleiern und so die Aufdeckung der Erstellung verdächtiger Infrastruktur zu vermeiden.

Umsetzbare Insights

1. Implementieren Sie eine gute Cyberhygiene, und schulen Sie Ihre Mitarbeiter in Bezug auf Cybersicherheit mit einer Anleitung, wie sie es vermeiden, Opfer von Social Engineering zu werden.
2. Führen Sie regelmäßige, automatisierte Überprüfungen auf Anomalien bei den Benutzeraktivitäten durch. Dies sollte durch Überwachung in großem Maßstab erfolgen, um Angriffe dieser Art zu reduzieren.
3. Aktualisieren und schützen Sie Router in Unternehmens- und privaten Netzwerken.

Ist Hacktivismus ein bleibendes Phänomen?

Auch wenn Hacktivismus kein neues Phänomen ist, erzeugte der Krieg in der Ukraine eine Flut von freiwilligen Hacker*innen, darunter einige, die von Regierungen gesteuert wurden, um den Ruf oder die Ressourcen von politischen Gegnern, Organisationen oder sogar Nationalstaaten zu beschädigen.

Im Februar 2022 forderte die ukrainische Regierung Zivilisten auf der ganzen Welt auf, als Teil der ukrainischen 300.000 Menschen starken „IT Army" Cyberattacken auf Russland durchzuführen.[33] Gleichzeitig begannen etablierte Hacktivisten-Gruppen wie Anonymous, Ghostsec, Against the West, Belarusian Cyber Partisans und RaidForum2 mit Angriffen zur Unterstützung der Ukraine. Andere Gruppen, darunter einige aus der Conti Ransomware-Bande, schlugen sich auf die Seite Russlands.[34]

In den folgenden Monaten waren die Aktivitäten von Anonymous deutlich sichtbar. Hacker*innen, die im Namen der Gruppe – oder einer ihrer Partner – agierten, legten vorübergehend Tausende russischer oder belarussischer Websites lahm, ließen Hunderte Gigabyte gestohlener Daten durchsickern, hackten russischen TV-Sender, um pro-ukrainische Inhalte abzuspielen, und boten sogar russischen Panzern, die sich ergaben, Zahlungen in Bitcoin an.

Das Aufkommen des Citizen-Hackers

Social Media-Plattformen ermöglichten die schnelle Organisation und Mobilisierung Tausender angehender Citizen-Hacker*innen, die eine Anleitung für einfach durchzuführende Angriffe erhielten, wie z. B. DDoS-Angriffe. Die Organisatoren nutzten Twitter, Telegram und private Foren, um Hacker zu versammeln, Prozesse zu organisieren und Hacking-Anleitungen zu verbreiten.

Allerdings dürften diese Hacker trotz aller Anleitungen nur über begrenzte Fähigkeiten verfügen. Dies legt zwei mögliche Entwicklungen in der Zukunft nahe: Erstens, Hunderttausende Individuen mit rudimentären technischen Fähigkeiten führen mithilfe von Angriffsvorlagen koordinierte oder individuelle Hacktivist-Angriffe gegen Ziele durch, oder, zweitens, beim letztendlichen Ende der kriegerischen Handlungen in der Ukraine lassen sie den Hacktivismus hinter sich, zumindest, bis das nächste politische oder soziale Problem sie zu neuen Taten inspiriert.

Politisierung von Hackern

Das größere Risiko dieser politischen Mobilisierung besteht im Einsatz technisch versierter Hacker, die möglicherweise weiterhin Cyberattacken gegen ausländische Regierungsziele durchführen, um ihre eigenen nationalen Prioritäten zu unterstützen, sei es auf eigene Faust oder im Auftrag ihrer Regierung.

Iran, China und Russland nutzen Hacktivismus bereits, um neue Kräfte für ihre staatlichen Hackergruppen zu rekrutieren. Beispielsweise hat die pro-russische Hackergruppe Killnet im April 2022 DDoS-Angriffe auf die tschechische Eisenbahn, regionale Flughäfen und die öffentliche Verwaltung Tschechiens durchgeführt, obwohl das Land gar nicht direkt am Krieg beteiligt ist.[35] Gleichzeitig könnten einige Regierungen Hacktivismus als Deckmantel für herkömmliche Spionage- oder Sabotageaktionen nutzen, z. B. iranische Aktionen gegen Israel.

In einem Umfeld vermehrter DDoS-Angriffe, die mit Hacktivismus in Verbindung stehen, ist die Technologiebranche herausgefordert, den Unterschied zwischen normalem und unnormalen Datenverkehrsfluss zu einer Webseite schnell zu erkennen. Microsoft und seine Partner haben eine Sammlung von Tools entwickelt, die den bösartigen DDoS-Datenverkehr erkennen und zu seinem Ursprung zurückverfolgen können. Darüber hinaus kann die Azure-Plattform von Microsoft Computer auf der Plattform identifizieren, die ein ungewöhnlich hohes Aufkommen von ausgehendem Datenverkehr erzeugen, und sie stilllegen.

Das Aufkommen von Protestware

Protestware hat sich als direkte Folge der emotionalen Reaktionen auf den Krieg zwischen Russland und der Ukraine entwickelt. Einige Entwickler*innen von Open Source-Software nutzten die Popularität ihrer Software als Mittel, um sich zu äußern oder gegen eine sich entwickelnde politische Situation aktiv zu werden. Dazu gehörten harmlose Textdateien, die auf einem Desktop oder in einem Browser geöffnet wurden, um Botschaften des Friedens zu verbreiten, aber auch gezielte Angriffe anhand der Geolokalisierung von IP-Adressen und destruktive Maßnahmen wie das Löschen einer Festplatte. Bei der Entwicklung weiterer globaler Ereignisse ist davon auszugehen, dass Protestware auch zukünftig wieder in Erscheinung treten wird. Da es sich in der Regel um Fälle handelt, in denen sich renommierte Open Source-Betreiber dazu entschließen, persönliche Statements über ihre eigenen Open Source-Komponenten zu machen, gibt es derzeit keinen Schutz, der diese Arten von Änderungen in den Quelldateipaketen verhindern könnte, und die Benutzer*innen sollten sich der möglichen Auswirkungen bewusst sein.

Social Media-Plattformen ermöglichten die Organisation und Mobilisierung Tausender angehender Citizen-Hacker, die eine Anleitung für einfach durchzuführende Angriffe erhielten, wie z. B. DDoS-Angriffe.

Umsetzbare Insights

1. Die Technologiebranche muss zusammenkommen, um eine umfassende Antwort auf diese neue Bedrohung zu entwickeln.
2. Führende Technologieunternehmen, einschließlich Microsoft, verfügen über Tools, um bösartigen Datenverkehr im Zusammenhang mit DDoS-Angriffen zu identifizieren und die verantwortlichen Computer zu deaktivieren.
3. In Zeiten geopolitischer Auseinandersetzungen sollten Open Source-Benutzer*innen besonders wachsam sein.

Fußnoten

1. https://www.reuters.com/business/energy/shell-re-routes-oil-supplies-after-cyberattack-german-logistics-firm-2022-02-01/
2. https://www.bleepingcomputer.com/news/security/greeces-public-postal-service-offline-due-to- ransomware-attack/
3. https://www.bleepingcomputer.com/news/security/costa-rica-s-public-health-agency-hit-by-hive-ransomware/; https://www.reuters.com/world/americas/cyber-attack-costa-rica-grows-more-agencies-hit-president-says-2022-05-16/
4. https://www.bleepingcomputer.com/news/security/spicejet-airline-passengers-stranded-after-ransomware-attack/
5. https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/
6. Erkennung und Reaktion am Endpunkt. https://www.microsoft.com/en-us/security/business/threat-protection/
7. https://www.washingtonpost.com/national-security/cyber-command-revil-ransomware/2021/11/03/528e03e6-3517-11ec-9bc4-86107e7b0ab1_story.html
8. https://www.bbc.com/news/technology-59998925
9. Ein geprüftes Forum ist ein Online-Diskussionsforum, in dem ein vorhandenes Mitglied für die Aufnahme eines neuen Mitglieds bürgen muss.
10. https://www.statista.com/statistics/800426/worldwide-blockchain-solutions-spending/; https://www.blockchain.com/charts/my-wallet-n-users; https://coinmarketcap.com
11. https://blogs.microsoft.com/on-the-issues/2022/04/13/zloader-botnet-disrupted-malware-ukraine/
12. https://www.coindesk.com/business/2021/12/13/crypto-exchange-ascendex-hacked-losses-estimated-at-77m/; https://www.zdnet.com/article/after-77-million-hack-crypto-platform-ascendex-to-reimburse-customers/
13. https://etherscan.io/address/0x73326b6764187b7176ed3c00109ddc1e6264eb8b
14. https://finance.yahoo.com/news/ethereum-worth-over-1-5m-160249300.html
15. https://news.bitcoin.com/decentralized-finance-crypto-exchange-uniswap-starts-blocking-addresses-linked-to-blocked-activities/
16. Datenquelle: Defender for Office (böswillige E-Mail/Aktivität von kompromittierter Identität), Azure Active Directory Identity Protection (Ereignisse mit kompromittierter Identität/ Warnungen), Defender for Cloud Apps (Ereignisse von Datenzugriff mit kompromittierter Identität) und M365D (produktübergreifende Korrelation).
17. Datenquelle: Defender for Endpoint (Angriffsverhalten Warnungen/Ereignisse), Defender for Office (böswillige E-Mail) und M365D (produktübergreifende Korrelation).
18. https://www.ic3.gov/Media/Y2022/PSA220504
19. DMARC (Domain-based Message Authentication, Reporting and Conformance): Eine Richtlinie zur Authentifizierung von E-Mails und ein Reporting-Protokoll, das darauf ausgelegt ist, Besitzer*innen von E-Mail-Domänen in die Lage zu versetzen, ihre Domäne vor unautorisierter Verwendung zu schützen.
20. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
21. https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/learn-about-spoof-intelligence?view=o365-worldwide
22. https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/impersonation-insight?view=o365-worldwide
23. https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-smartscreen/microsoft-defender-smartscreen-overview
24. https://www.microsoft.com/en-us/security/business/siem-and-xdr/microsoft-defender-office-365
25. https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-smartscreen/microsoft-defender-smartscreen-overview
26. Microsoft Corporation v. John Does 1-27, et al., Nr. 1:10CV156, (E.D.Va. 22. Feb. 2010).
27. Siehe Bowden, Mark. Worm: The First Digital World War. Grove/Atlantic, Inc., 27. Sept. 2011.
28. Insbesondere Regel 65 der US-amerikanischen Zivilprozessordnung ermöglicht es einer Partei, ein solches Rechtsmittel zu suchen, wenn: 1) die Partei unmittelbare und irreparable Schäden erleiden wird, falls die Entlastung nicht gewährt wird, und 2) die Partei versucht, die andere Seite fristgerecht zu informieren. Darüber hinaus verlangt das Gesetz die Anwendung einer Ausgleichsprüfung, bei der das Recht des Beklagten, informiert zu werden, gegen den Schaden für die Öffentlichkeit abgewogen wird.
29. Microsoft Corporation v. John Does 1-11, et al., Nr. 2:11cv222, (W.D. Wa. 9. Feb. 2011).
30. Microsoft Corp. v. Does, Nr. 1:20-cv-01171 (AJT/IDD), 2021 U.S. Dist. LEXIS 258143, at *1 (E.D. Va. 12. Aug. 2021).
31. https://github.com/microsoft/routeros-scanner
32. RiskIQ: Ubiquiti Devices Compromised and Used as Malware C2 Reverse Proxies | RiskIQ Community Edition
33. https://www.theguardian.com/world/2022/mar/18/amateur-hackers-warned-against-joining-ukraines-it-army
34. https://therecord.media/russia-or-ukraine-hacking-groups-take-sides/
35. https://www.expats.cz/czech-news/article/pro-russian-hackers-target-czech-websites-in-a-series-of-attacks

Bedrohungen durch Nationalstaaten

Nationalstaatliche Akteure führen immer ausgefeiltere Cyberattacken durch, um eine Erkennung zu umgehen und ihre strategischen Prioritäten voranzutreiben.

Eine Übersicht über

Bedrohungen durch Nationalstaaten

Nationalstaatliche Akteure führen immer ausgefeiltere Cyberattacken durch, um eine Erkennung zu umgehen und ihre strategischen Prioritäten voranzutreiben. Mit dem Einsatz von Cyberwaffen im hybriden Krieg in der Ukraine bricht ein neues Konfliktzeitalter an.

Russland hat seinen Krieg auch mit Operationen zur Informationsbeeinflussung flankiert. Dabei nutzte es Propaganda zur Einflussnahme auf Meinungen in Russland, in der Ukraine und weltweit. Dieser erste umfassende hybride Konflikt hat uns weitere wichtige Lektionen gelehrt. Erstens: Der beste Schutz für die Sicherheit digitaler Prozesse und Daten – sowohl im Cyberspace als auch im physischen Raum – ist der Umstieg auf die Cloud. Die ersten russischen Angriffe zielten mithilfe von Wiper-Schadsoftware auf On-Premises-Dienste, und eine der ersten Raketen, die überhaupt gestartet wurden, zielte auf physische Rechenzentren.

Die Ukraine reagierte mit einer schnellen Verlagerung von Workloads und Daten in hyperskalierte Clouds, die in Rechenzentren außerhalb der Ukraine gehostet wurden. Zweitens: Die Fortschritte bei Threat Intelligence und Endpunktschutz, die den Daten und leistungsstarken KI- und ML-Diensten in der Cloud zu verdanken sind, kamen der Ukraine bei der Verteidigung gegen russische Cyberattacken zugute.

Andernorts haben nationalstaatliche Akteure ihre Aktivität ausgeweitet und nutzen technologische Fortschritte bei Automatisierung, Cloud-Infrastruktur und Remote-Zugriff für Angriffe auf eine breitere Palette von Zielen. Häufiges Angriffsziel waren IT-Lieferketten von Unternehmen, die einen Zugriff auf die letztendlichen Ziele ermöglichten. Cyberhygiene wurde noch wichtiger, weil die Akteure ungepatchte Schwachstellen schnell ausnutzten, sowohl ausgefeilte als auch Brute-Force-Techniken nutzten, um Anmeldeinformationen zu stehlen, und ihre Aktionen mithilfe von Open Source oder legitimer Software verschleierten. Und der Iran verbündet sich bei der Nutzung destruktiver Cyberwaffen mit Russland. Das schließt auch Ransomware als Grundpfeiler ihrer Angriffe mit ein.

Diese Entwicklungen erfordern die dringende Einführung eines einheitlichen, globalen Rahmens, der die Menschenrechte priorisiert und Menschen vor rücksichtslosem staatlichen Verhalten im Cyberraum schützt. Alle Nationen müssen zusammenarbeiten, um vereinbarte Normen und Regeln für ein verantwortungsvolles staatliches Verhalten zu implementieren.

› Defending Ukraine: Early Lessons from the Cyber War – Microsoft On the Issues

Verstärkte Angriffe auf kritische Infrastruktur, insbesondere IT-Sektor, Finanzdienstleistungen, Transportsysteme und Kommunikationsinfrastruktur.

› Weitere Informationen finden Sie auf S. 35

Die IT-Lieferkette wird als Gateway für den Zugriff auf Ziele verwendet.

NOBELIUM

› Weitere Informationen finden Sie auf S. 36

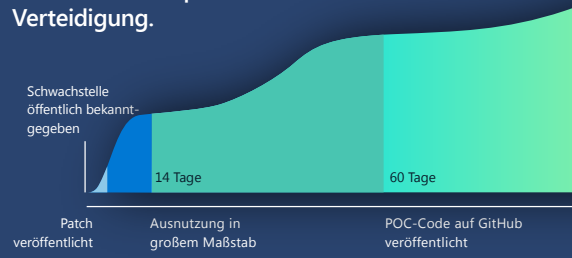
China verstärkt die weltweiten Angriffe, insbesondere auf kleinere Länder in Südostasien, um Informationen und Wettbewerbsvorteile zu gewinnen.

› Weitere Informationen finden Sie auf S. 44

Iran wurde nach dem Machtwechsel zunehmend aggressiver, weitete Ransomware-Angriffe über regionale Kontrahenten hinweg auf Opfer in den USA und in der EU aus und nahm prominente kritische Infrastruktur in den USA ins Ziel.

› Weitere Informationen finden Sie auf S. 46

Die Identifizierung und schnelle Ausnutzung von ungepatchten Schwachstellen ist zu einer wichtigen Taktik geworden. Die schnelle Bereitstellung von Sicherheitsupdates ist ein Schlüssel zur Verteidigung.



› Weitere Informationen finden Sie auf S. 39

Nordkorea griff Rüstungs- und Luftfahrtunternehmen, Kryptowährungsanbieter, Nachrichtenagenturen, Überläufer und Hilfsorganisationen an, um die Ziele des Regimes zu erreichen: Aufbau der Verteidigung, Stärkung der Wirtschaft und Sicherstellung der inneren Stabilität.

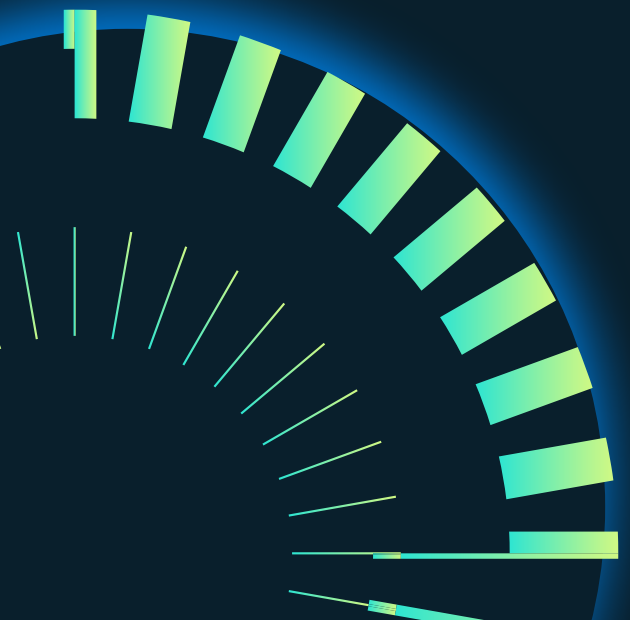
› Weitere Informationen finden Sie auf S. 49

Cybersöldner*innen bedrohen die Stabilität des Cyberspace, da diese wachsende Branche privater Unternehmen fortschrittliche Tools, Techniken und Dienste entwickelt und verkauft, damit ihre Kunden (häufig Regierungen) in Netzwerke und Geräte eindringen können.

› Weitere Informationen finden Sie auf S. 52

Einführung

Nach hochkarätigen Angriffen in den Jahren 2020 und 2021 haben nationalstaatliche Akteure erhebliche Ressourcen in die Anpassung an neue Sicherheitsmaßnahmen gesteckt, die von Organisationen zur Verteidigung gegen ausgefeilte Bedrohungen implementiert wurden.



Ähnlich wie Unternehmensorganisationen begannen die Gegner damit, Fortschritte in den Bereichen Automatisierung, Cloud-Infrastruktur und RAS-Technologien für die Ausweitung ihrer Angriffe zu nutzen. Diese taktischen Anpassungen führten zu neuen Ansätzen und groß angelegten Angriffen auf Unternehmenslieferketten. Die Hygiene zum Aufrechterhalten von IT-Sicherheit hat einen noch höheren Stellenwert erlangt, weil die Akteure neue Methoden zum Ausnutzen ungepatchter Schwachstellen entwickelt, Techniken zum Kompromittieren von Unternehmensnetzwerken ausgebaut und ihre Aktivitäten mithilfe von Open Source- oder legitimer Software verschleiert haben. Neue Angriffstechniken sorgten für neue und schwerer zu entdeckende Vektoren, um auf das Netzwerk eines Ziels zuzugreifen. Als schließlich die physischen Angriffe des Krieges eskalierten, beobachteten wir, dass Cyberattacken eine herausragende Rolle bei den militärischen Aktivitäten einnahmen.

Der Konflikt in der Ukraine hat ein allzu schmerzliches Beispiel dafür geliefert, wie sich Cyberangriffe weiterentwickeln, um – parallel zu den militärischen Konflikten am Boden – Einfluss in der Welt auszuüben. Energie- und Telekommunikationssysteme, Medien und andere kritische Infrastrukturen wurden zu Zielen sowohl physischer Angriffe als auch von Cyberattacken. Die Versuche zum Kompromittieren von Netzwerken, die als Teil von Spionagekampagnen und Kampagnen zum Exfiltrieren von Daten beobachtet wurden, fokussierten sich im hybriden Krieg auf Angriffe mit Wiper-Schadsoftware gegen kritische Infrastruktursysteme. Die Vernetzung der Sicherheit solcher Systeme mit der Cloud führte zu einer frühzeitigen Erkennung und Unterbindung potenziell verheerender Angriffe.[1]

Zum ersten Mal hat ML-gestützte Verhaltenserkennung in einem großen Cyberevent Angriffe über bekannte Angriffsmuster ohne vorherige Kenntnis der zugrunde liegenden Schadsoftware erfolgreich erkannt und weitere verhindert – noch bevor Menschen die Bedrohungen überhaupt bemerkten. Wir fanden auch bestätigt, welche wichtige Rolle der Echtzeitaustausch von Threat Intelligence mit Verteidigern beim Schutz dieser Systeme spielt. Sie erhalten auf diesem Wege die lebenswichtigen Informationen, die sie benötigen, um diese Angriffe zu antizipieren und sich gegen sie zu verteidigen.

Nationalstaatliche Akteure auf der ganzen Welt bauen ihre Aktivitäten mit alten und neuen Vorgehensweisen weiter aus. China, Nordkorea, Iran und Russland haben allesamt Angriffe auf Microsoft-Kund*innen durchgeführt. Die IT-Services-Lieferkette wurde zu einem beliebten Ziel, weil die Akteure den Fokus auf vorgelagerte Dienste verlagerten, die als Zugriffspunkte auf gleich mehrere Organisationen dienen können. Wir gehen davon aus, dass die Akteure damit fortfahren, vertrauenswürdige Beziehungen in den Lieferketten von Unternehmen auszunutzen. Dies unterstreicht die Bedeutung einer umfangreichen Durchsetzung von Authentifizierungsregeln, von lückenlosem Patchen, von Kontenkonfiguration für die Remote-Zugriffsinfrastruktur und von regelmäßigen Prüfungen der Partnerbeziehungen in Hinblick auf die Authentizität.

Wie auch Betreiber von Ransomware und andere Cyberkriminelle haben nationalstaatliche Akteure auf die verstärkte Exposition reagiert. Daher haben sie sich auf schlecht konfigurierte oder ungepatchte Unternehmenssysteme (VPN-/VPS-Infrastruktur, On-Premises-Server, Software von Drittanbietern) verlagert und verfolgen dort „Living-off-the-Land"-Angriffe. Viele haben den Einsatz von Standardschadsoftware und Open Source-Tools von Roten Teams beim Verschleiern ihrer bösartigen Aktivitäten ausgeweitet.

Zur Aufrechterhaltung einer soliden IT-Sicherheitshygiene zählen Maßnahmen wie priorisiertes Patchen, Funktionen für den Manipulationsschutz, Tools zur Verwaltung von Angriffsoberflächen wie RiskIQ, die eine Außenansicht von Angriffsoberflächen liefern, und die Aktivierung von Multi-Faktor-Authentifizierung im gesamten Unternehmen. All dies sind mittlerweile Grundlagen für eine proaktive Verteidigung gegen viele höchst raffinierte Akteure.

Als Taktik bei ihren Angriffen haben nationalstaatliche Akteure auch den Einsatz von Ransomware verstärkt. Häufig wird dabei Ransom-Schadsoftware wiederverwendet, die bei ihren Angriffen von der kriminellen Infrastruktur erzeugt wurde. Wir haben sowohl bei Angreifern aus dem Iran als auch aus Nordkorea beobachtet, wie sie vorkonfektionierte Ransomware-Tools zum Beschädigen der anvisierten Systeme regionaler Rivalen einsetzten. Dies umfasste häufig auch kritische Infrastruktur. Schließlich wurden wir Zeuge der wachsenden Bedrohung durch Cybersöldner, die Tools, Techniken und Services für die zunehmende Ausnutzung der Schwachstellen von Drittunternehmen entwickeln und verkaufen. Die Komplexität und Agilität von Angriffen durch nationalstaatliche Akteure wird sich auch in Zukunft von Jahr zu Jahr weiterentwickeln. Organisationen müssen darauf reagieren, indem sie sich über die Änderungen dieser Akteure informieren und gleichzeitig ihre Verteidigung ausbauen.

John Lambert
Corporate Vice President und Distinguished Engineer, Microsoft Threat Intelligence Center

Hintergrund zu Daten über Nationalstaaten

Bedrohungen durch Nationalstaaten sind als bedrohliche Cyberaktivitäten definiert, die ihren Ursprung in einem bestimmten Land haben und die offensichtliche Absicht verfolgen, nationalen Interessen zu dienen. Nationalstaatliche Akteure bilden einige der fortschrittlichsten und hartnäckigsten Bedrohungen, denen unsere Kund*innen gegenüberstehen. Dies umfasst auch den Diebstahl von geistigem Eigentum, Spionage, Überwachung, Diebstahl von Anmeldeinformationen, destruktive Angriffe und vieles mehr.

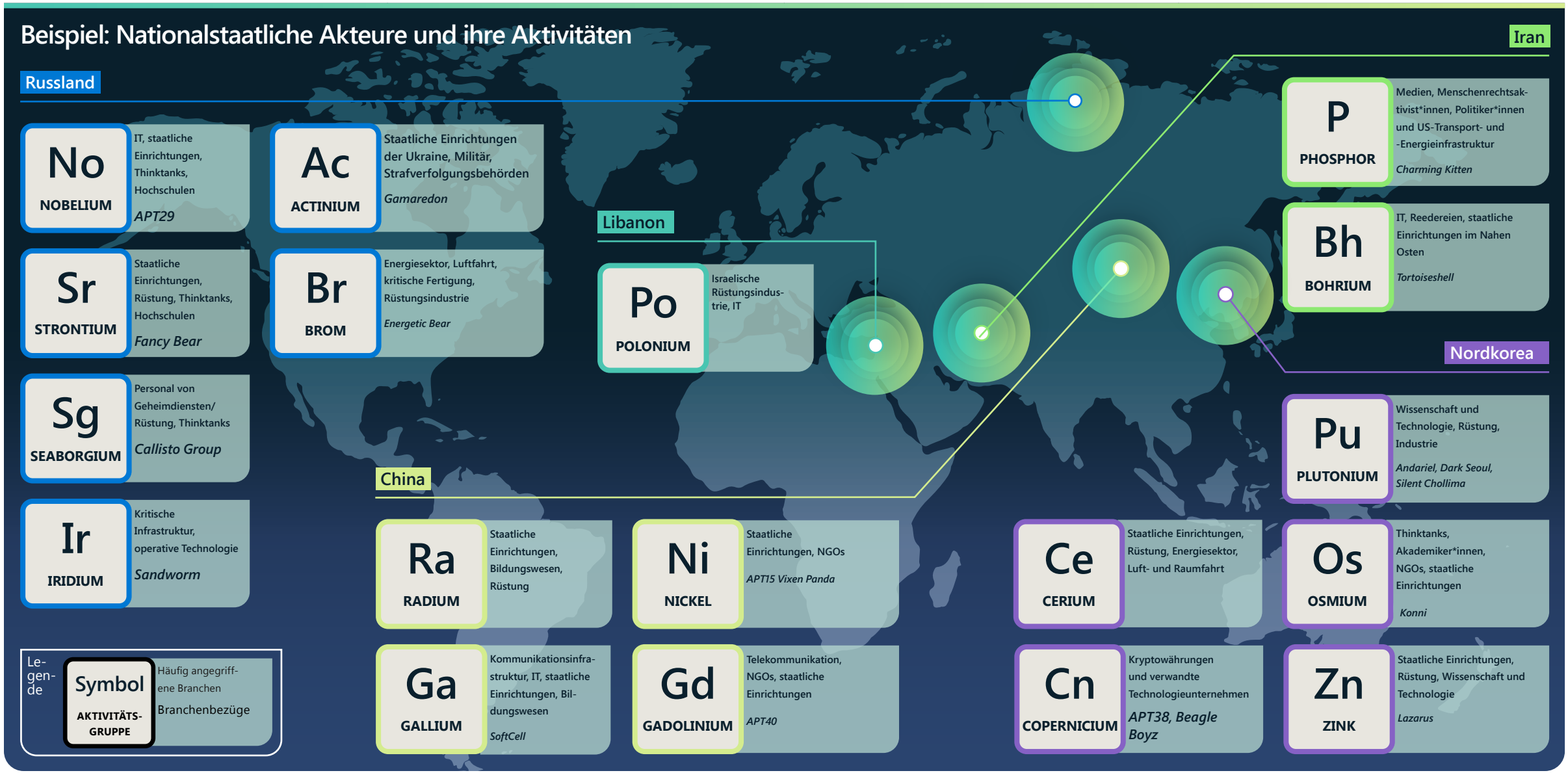
Wir investieren erhebliche Ressourcen in die Aufdeckung, das Verstehen und die Abwehr dieser Bedrohungen. Werden Organisationen oder einzelne Kontoinhaber*innen durch beobachtete nationalstaatliche Aktivitäten ins Ziel genommen oder kompromittiert, sendet Microsoft den entsprechenden Kund*innen eine direkte Benachrichtigung (Nation State Notification, NSN). Sie enthält die Informationen, die sie benötigen, um die jeweilige Aktivität zu untersuchen. Seit den Anfängen im Jahr 2018 haben wir bis Juni 2022 über 67.000 NSNs versendet.

Die Daten der Microsoft NSN-Warnungen werden in diesem Kapitel vorgestellt, um eine Übersicht über messbare Aktivitäten zu bieten. Der in den Diagrammen dargestellte Aktivitätsgrad basiert auf der Anzahl von NSNs, die Microsoft an seine Kund*innen gesendet hat, wenn festgestellt wurde, dass mindestens ein Konto in deren Organisation von staatlichen Akteuren attackiert oder kompromittiert wurde.

Die vier primären Nationalstaaten, deren Bedrohungsgruppen wir in diesen Bericht aufgenommen haben, sind Russland, China, Iran und Nordkorea. Dabei handelt es sich um die Herkunftsländer der am häufigsten beobachteten Akteure, die Microsoft-Kund*innen im letzten Jahr angegriffen haben. Der Bericht enthält außerdem unsere Beobachtungen über Bedrohungsgruppen aus dem Libanon und von Cybersöldnern oder offensiven bezahlten Akteuren im privaten Sektor.

Microsoft bezeichnet nationalstaatliche Gruppen mit den Namen chemischer Elemente (z. B. NOBELIUM), von denen nur einige auf der folgenden Seite präsentiert werden. Unbekannte, aufkommende oder sich entwickelnde Cluster von Bedrohungsaktivität bezeichnen wir nach dem Muster DEV-####. Damit können wir diese Entitäten als einen eindeutigen Satz von Informationen verfolgen, bis wir genauere Erkenntnisse über die Herkunft oder die Identität der dahinter stehenden Akteure gewonnen haben.

Sobald die Kriterien erfüllt sind, wird ein DEV in einen benannten Akteur umgewandelt oder bestehenden Akteuren zugeordnet. Im ganzen folgenden Kapitel geben wir Beispiele für nationalstaatliche und DEV-Gruppen, um einen tieferen Einblick in Bezug auf Angriffsziele und Techniken sowie eine Analyse der Motivationen zu liefern. Obwohl viele dieser Gruppen die gleichen Tools wie Cyberkriminelle verwenden, stellen sie durch maßgeschneiderte Schadsoftware, die Möglichkeit zum Entdecken und Ausnutzen von Zero-Day-Schwachstellen und durch ihre Straffreiheit eine einzigartige Form der Bedrohung dar.


Beispiel: Nationalstaatliche Akteure und ihre Aktivitäten
Russland
No
NOBELIUM
IT, staatliche Einrichtungen, Thinktanks, Hochschulen
APT29
Ac
ACTINIUM
Staatliche Einrichtungen der Ukraine, Militär, Strafverfolgungsbehörden
Gamaredon
Sr
STRONTIUM
Staatliche Einrichtungen, Rüstung, Thinktanks, Hochschulen
Fancy Bear
Br
BROM
Energiesektor, Luftfahrt, kritische Fertigung, Rüstungsindustrie
Energetic Bear
Sg
SEABORGIUM
Personal von Geheimdiensten/ Rüstung, Thinktanks
Callisto Group
Ir
IRIDIUM
Kritische Infrastruktur, operative Technologie
Sandworm
Libanon
Po
POLONIUM
Israelische Rüstungsindustrie, IT
China
Ra
RADIUM
Staatliche Einrichtungen, Bildungswesen, Rüstung
Ni
NICKEL
Staatliche Einrichtungen, NGOs
APT15 Vixen Panda
Ga
GALLIUM
Kommunikationsinfrastruktur, IT, staatliche Einrichtungen, Bildungswesen
SoftCell
Gd
GADOLINIUM
Telekommunikation, NGOs, staatliche Einrichtungen
APT40
Iran
P
PHOSPHOR
Medien, Menschenrechtsaktivist*innen, Politiker*innen und US-Transport- und -Energieinfrastruktur
Charming Kitten
Bh
BOHRIUM
IT, Reedereien, staatliche Einrichtungen im Nahen Osten
Tortoiseshell
Nordkorea
Pu
PLUTONIUM
Wissenschaft und Technologie, Rüstung, Industrie
Andariel, Dark Seoul, Silent Chollima
Ce
CERIUM
Staatliche Einrichtungen, Rüstung, Energiesektor, Luft- und Raumfahrt
Os
OSMIUM
Thinktanks, Akademiker*innen, NGOs, staatliche Einrichtungen
Konni
Cn
COPERNICIUM
Kryptowährungen und verwandte Technologieunternehmen
APT38, Beagle Boyz
Zn
ZINK
Staatliche Einrichtungen, Rüstung, Wissenschaft und Technologie
Lazarus
Legende
Symbol
AKTIVITÄTS-GRUPPE
Häufig angegriffene Branchen
Branchenbezüge

Die Entwicklung der Bedrohungslandschaft

Die Mission von Microsoft, nationalstaatliche Akteure nachzuverfolgen, wenn wir feststellen, dass unsere Kund*innen ins Ziel genommen oder kompromittiert werden, ist tief in unserer Aufgabe verankert, Anwender*innen vor Angriffen zu schützen.

Diese Benachrichtigung ist ein wesentlicher Bestandteil unserer Selbstverpflichtung, unsere Kunden darüber zu informieren, ob beobachtete Angriffe durch den Schutz unserer Sicherheitsprodukte erfolgreich verhindert wurden oder ob sie aufgrund unbekannter Sicherheitsschwachstellen Wirkung entfalten konnten. Durch das Nachverfolgen von Benachrichtigungen über einen bestimmten Zeitraum hinweg kann Microsoft entstehende Bedrohungstrends nach Akteur identifizieren und die Schutzfunktionen darauf abstimmen, die Bedrohungen gegen unsere Kund*innen auf all unseren Cloud-Diensten zu verringern.

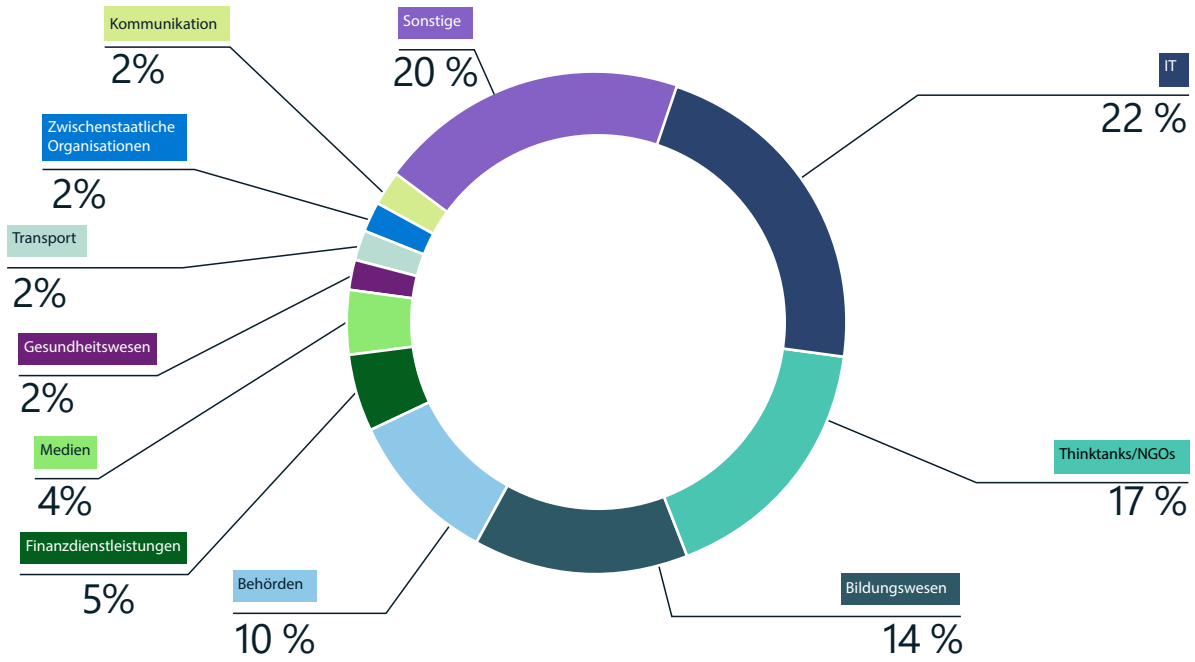
Mit dieser Nachverfolgung können wir Daten und Insights über unsere Beobachtungen weitergeben. Die Analyst*innen, die diese Akteure beobachten und ihren Angriffen folgen, stützen sich auf eine Kombination aus technischen Indikatoren und geopolitischer Expertise, um die Motivationen der Akteure zu verstehen. Dabei kombinieren sie technische und globale Zusammenhänge zu neuen Insights. Diese Art der Kuratierung bietet einen einzigartigen Einblick in die Prioritäten von nationalstaatlichen Cyberakteuren und liefert Erkenntnisse darüber, wie ihre Motivationen die politischen, militärischen und wirtschaftlichen Prioritäten der Nationalstaaten, von denen sie engagiert werden, widerspiegeln.

Die politischen Entwicklungen im vergangenen Jahr prägten weltweit die Prioritäten und die Risikotoleranz von staatlich geförderten Bedrohungsgruppen. Mit dem Zusammenbrechen geopolitischer Beziehungen und dem steigenden Einfluss der Hardliner in einigen Ländern wurden Cyberakteure zunehmend mutiger und aggressiver. Zum Beispiel:

- Russland hat staatliche Einrichtungen der Ukraine und die kritische Infrastruktur des Landes unerbittlich angegriffen, um die Bodenoperationen seines Militärs zu flankieren.[2]
- Der Iran suchte aggressiv nach Einfallstoren in kritische US-Infrastruktur, z. B. Hafenbehörden.
- Nordkorea setzte seine Kampagne zum Diebstahl von Kryptowährung von Finanz- und Technologieunternehmen fort.
- China hat seine globalen Aktivitäten zur Cyberspionage ausgeweitet.

Auch wenn nationalstaatliche Akteure technisch anspruchsvoll sein mögen und eine Vielzahl von Taktiken einsetzen, können ihre Angriffe oft durch eine gute Cyberhygiene abgeschwächt werden. Viele dieser Akteure verlassen sich auf technisch relativ unaufwändige Mittel wie Spear-Phishing-E-Mails zum Einschleusen ausgefeilter Schadsoftware, anstatt zum Erreichen ihrer Ziele in die Entwicklung maßgeschneiderter Exploits zu investieren oder gezielt Social Engineering zu betreiben.

Von nationalstaatlichen Akteuren angegriffene Industriezweige



Nationalstaatliche Gruppen haben sich auf eine Reihe von Sektoren konzentriert. Russische und iranische Akteure haben die IT-Branche als Einfallstor für den Zugriff auf die Kund*innen der jeweiligen IT-Unternehmen ins Ziel genommen. Thinktanks, Nichtregierungsorganisationen (NGOs), Universitäten und Regierungsbehörden blieben weiterhin gemeinsame Ziele nationalstaatlicher Akteure.

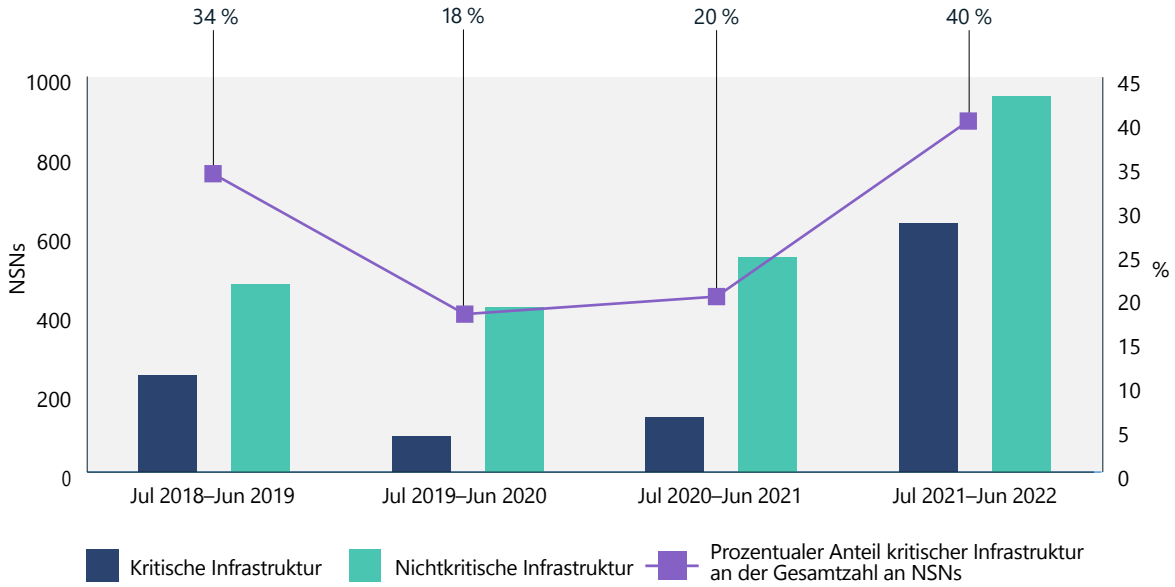
Nationalstaatliche Akteure haben viele unterschiedliche Ziele. Dies kann dazu führen, dass spezielle Gruppen von Organisationen oder Einzelpersonen ins Visier genommen werden. Im letzten Jahr haben sich die Angriffe auf die Lieferkette erhöht. Dabei lag der Fokus besonders auf IT-Unternehmen. Durch die Kompromittierung von IT-Dienstleistern können Akteure ihr ursprüngliches Ziel häufig über eine vertrauenswürdige Beziehung mit dem Unternehmen erreichen, wenn sich diese auf die Verwaltung vernetzter Systeme bezieht.

Sie können Angriffe auch in einem weitaus größeren Maßstab ausführen, indem sie Hunderte nachgelagerter Kund*innen in einem einzigen Angriff kompromittieren. Nach dem IT-Sektor waren Thinktanks, Akademiker*innen in Verbindung mit Universitäten und Regierungsbeamte die häufigsten Ziele. All dies sind begehrte „weiche Ziele“ für Spionage, um Informationen zu geopolitischen Themen zu sammeln.

Die Entwicklung der Bedrohungslandschaft

Fortsetzung

Trends bei kritischer Infrastruktur

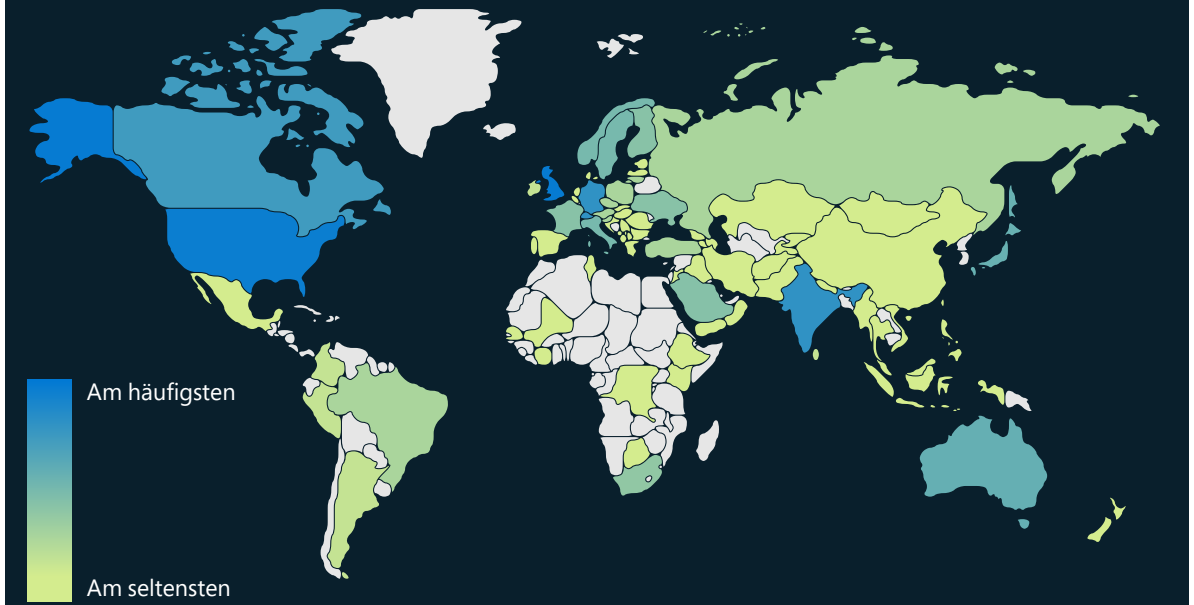


Im vergangenen Jahr hatten es nationalstaatliche Gruppen vermehrt auf kritische Infrastruktur[3] abgesehen. Dabei konzentrierten sie sich auf Unternehmen im IT-Sektor, Finanzdienstleistungen, Transportsysteme und Kommunikationsinfrastruktur.

„Vor der Invasion der Ukraine glaubten Regierungen, dass Daten in einem Land bleiben müssen, um sicher zu sein. Nach der Invasion ist die Migration von Daten in die Cloud und ihr Verschieben nach außerhalb des Staatsgebiets inzwischen ein Teil der Resilienzplanung und verantwortungsvollen Governance."

Cristin Flynn Goodwin,
Associate General Counsel, Customer Security & Trust

Geografische Ausrichtung der nationalstaatlichen Akteure



Die Ziele waren im vergangenen Jahr über den ganzen Globus verteilt, aber ein besonderer Fokus lag auf US-amerikanischen und britischen Unternehmen. Unternehmen in Israel, den VAE, Kanada, Deutschland, Indien, der Schweiz und Japan gehörten nach unseren NSN-Daten ebenfalls zu den häufigsten Zielen.

Umsetzbare Insights

1. Identifizieren und schützen Sie Ihre potenziell hochwertigen Daten, gefährdete Technologien, Informationen und Geschäftsprozesse, die zu den strategischen Prioritäten nationalstaatlicher Gruppen passen könnten.
2. Aktivieren Sie Cloud-Schutzfunktionen, um bekannte und neuartige Bedrohungen für Ihr Netzwerk im großen Maßstab zu identifizieren und zu reduzieren.

Die IT-Lieferkette als Zugang zur digitalen Infrastruktur

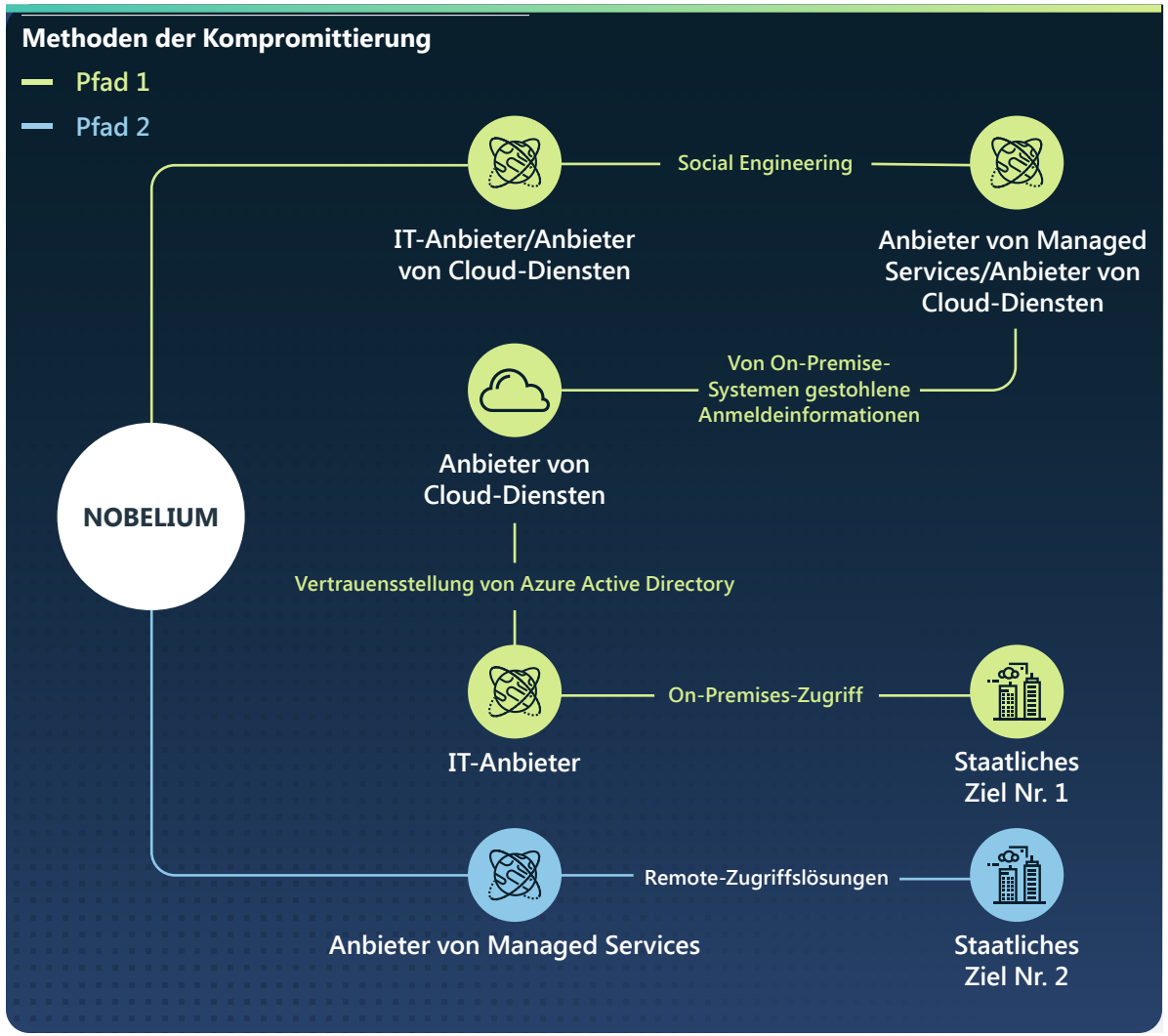
Über die Angriffe von Nationalstaaten auf IT-Anbieter könnten die Akteure Gelegenheit zum Anvisieren weiterer Organisationen von Interesse erhalten, indem sie das Vertrauen und den Zugriff in und für diese Lieferkettenanbieter zu ihren Gunsten ausnutzen. Im vergangenen Jahr nutzten nationalstaatliche Gruppen IT-Dienstanbieter für den Angriff auf Drittziele sowie für den Zugriff auf nachgelagerte Opfer in staatlichen Einrichtungen, gesetzgebenden Instanzen und bei kritischer Infrastruktur.

IT-Dienstleister sind attraktive Zwischenziele, weil sie Hunderten von direkten und Tausenden von indirekten Klienten dienen, die für ausländische Nachrichtendienste von Interesse sind. Falls diese Systeme kompromittiert werden, könnten die routinemäßigen Geschäftspraktiken und die delegierten Administratorrechte, die diese Firmen genießen, bösartigen Akteuren ermöglichen, in die Klientennetzwerke von IT-Dienstanbietern einzudringen und sie zu manipulieren, ohne sofort Warnmeldungen auszulösen.

Im vergangenen Jahr versuchte NOBELIUM, privilegierte Konten bei Anbietern von Cloud-Lösungen und anderen Managed Services zu kompromittieren und auszunutzen, um möglichst Zugriff auf nachgelagerte US- und europäische Kunden bei staatlichen Stellen und gesetzgebenden Institutionen zu erlangen.

NOBELIUM zeigte, wie der Ansatz „kompromittiere einen, um viele zu kompromittieren“ gegen einen vermeintlichen geopolitischen Gegner gerichtet werden könnte. Im vergangenen Jahr drang der Akteur direkt oder über Dritte in sensitive Organisationen in Mitgliedstaaten der NATO ein. Die russische Regierung nimmt die NATO als eine existenzielle Bedrohung wahr. Zwischen Juli 2021 und Anfang Juni 2022 gingen 48 % der Kundenbenachrichtigungen von Microsoft über russische Bedrohungsaktivitäten gegen Kunden von Onlinediensten an Firmen im IT-Sektor in NATO-Mitgliedsstaaten. Vermutlich dienten diese als Zwischenzugriffspunkt. Insgesamt 90 % der Benachrichtigungen über russische Bedrohungsaktivitäten gingen im gleichen Zeitraum an Kund*innen in NATO-Mitgliedstaaten, vor allem in der IT, in Thinktanks, in Nichtregierungsorganisationen (NGOs) und in staatlichen Stellen. Dies lässt auf eine Strategie schließen, die mehrere Möglichkeiten des ersten Zugriffs auf diese Ziele verfolgt.

Es gab eine Verlagerung von der Ausnutzung der Softwarelieferkette hin zur Ausnutzung der IT-Services-Lieferkette, wobei Anbieter von Cloud-Lösungen und Managed Services als Zwischenstation für Angriffe auf nachgelagerte Kund*innen verwendet wurden.



Dieses Diagramm zeigt den Multivektoransatz von NOBELIUM beim Kompromittieren seiner endgültigen Ziele sowie die Kollateralschäden für andere Opfer entlang des Weges. Zusätzlich zu den oben gezeigten Aktionen startete NOBELIUM Kennwort-Spray- und Phishing-Angriffe gegen die beteiligten Entitäten. Dabei wurde sogar das persönliche Konto von mindestens eine/m Regierungsmitarbeiter*in angegriffen, was eine weitere potenzielle Kompromittierungsmöglichkeit bildete.

Die IT-Lieferkette als Zugang zur digitalen Infrastruktur

Fortsetzung

Über das ganze Jahr hinweg entdeckte das Microsoft Threat Intelligence Center (MSTIC) eine zunehmende Anzahl von staatlichen oder staatsnahen iranischen Akteuren, die IT-Unternehmen kompromittierten. In vielen Fällen wurden die Akteure dabei entdeckt, wie sie Anmeldeinformationen stahlen, um Zugriff auf nachgelagerte Entitäten für eine Reihe von Zielen zu nehmen: von der Sammlung von Informationen bis hin zu destruktiven Vergeltungsangriffen.

- Im Juli und August 2021 kompromittierte DEV-0228 einen israelischen Anbieter von Unternehmenssoftware, um später nachgelagerte Kund*innen in den Sektoren Rüstung, Energie und Rechtswesen in Israel zu kompromittieren.[4]
- Von August bis September 2021 entdeckte Microsoft einen Ausschlag bei staatlichen iranischen Akteuren, die IT-Unternehmen in Indien angriffen. Da es für diese Verlagerung keinedringenden geopolitischen Gründe gab, ist davon auszugehen, dass dies dem Ziel diente, indirekt auf Tochterunternehmen und Kund*innen außerhalb Indiens zuzugreifen.
- Im Januar 2022 kompromittierte DEV-0198, eine Gruppe, die unserer Meinung nach mit der iranischen Regierung in Zusammenhang steht, einen israelischen Anbieter von Cloud-Diensten. Nach Einschätzung von Microsoft nutzte der Akteur wahrscheinlich kompromittierte Anmeldeinformationen des Anbieters, um Zugriff auf ein israelisches Logistikunternehmen zu authentifizieren. Später im Monat beobachtete MSTIC den gleichen Akteur beim Versuch, einen destruktiven Cyberangriff gegen das Logistikunternehmen durchzuführen.
- Im April 2022 kompromittierte POLONIUM, eine im Libanon ansässige Gruppe, von der wir vermuten, dass sie mit staatlichen iranischen Gruppen an IT-Lieferkettentechniken zusammenarbeitete, ein weiteres israelisches IT-Unternehmen, um Zugriff auf israelische Organisationen in der Rüstungsindustrie und im Rechtswesen zu erhalten.[5]

Die Aktivitäten im vergangenen Jahr haben gezeigt, dass Akteure wie NOBELIUM und DEV-0228 die Vertrauensstellungslandschaft einer Organisation mit der Zeit besser kennen als die Organisationen selbst. Diese zunehmende Bedrohung unterstreicht, dass Unternehmen die Grenzen und Einstiegspunkte ihrer digitalen Ressourcen verstehen und verstärkt schützen müssen. Es verdeutlicht außerdem, wie wichtig es für IT-Dienstanbieter ist, den Status ihrer eigenen Cybersicherheit konsequent zu überwachen. So sollten Organisationen beispielsweise Multi-Faktor-Authentifizierung und Richtlinien für bedingten Zugriff implementieren, um es bösartigen Akteuren zu erschweren, privilegierte Konten zu erbeuten oder sich in einem Netzwerk auszubreiten.

Die Durchführung einer gründlichen Überprüfung und Überwachung von Partnerbeziehungen trägt dazu bei, alle unnötigen Berechtigungen zwischen Ihrer Organisation und vorgelagerten Anbietern zu minimieren und den Zugriff für alle unbekannten Beziehungen sofort zu entfernen. Eine bessere Vertrautheit mit Aktivitätsprotokollen und die Überprüfung der verfügbaren Aktivitäten erleichtern das Erkennen von Anomalien, die weitere Ermittlungen auslösen könnten.

> Indem Nationalstaaten Drittparteien ins Ziel nehmen, können sie sensible Organisationen durch Ausnutzung von Vertrauensstellungen und Zugriff innerhalb einer Lieferkette angreifen.

Umsetzbare Insights

1. Überprüfen und überwachen Sie Beziehungen zu vorgelagerten und nachgelagerten Anbietern sowie delegierte privilegierte Zugriffsrechte, um unnötige Berechtigungen zu minimieren. Entfernen Sie den Zugriff für alle Partnerbeziehungen, die unbekannt wirken oder noch nicht geprüft wurden.[6]
2. Aktivieren Sie die Protokollierung, und überprüfen Sie alle Authentifizierungsaktivitäten für die RAS-Infrastruktur und virtuelle private Netzwerke (VPNs). Konzentrieren Sie sich dabei auf Konten, die mit Single-Faktor-Authentifizierung konfiguriert sind, um die Authentizität zu bestätigen und anomale Aktivitäten zu untersuchen.
3. Aktivieren Sie MFA für alle Konten (einschließlich Dienstkonten), und stellen Sie sicher, dass MFA für sämtliche Remote-Verbindungen erzwungen wird.
4. Verwenden Sie passwortgeschützte Lösungen für den Schutz der Konten.[7]

Links zu weiteren Informationen

- NOBELIUM targeting delegated administrative privileges to facilitate broader attacks | Microsoft Threat Intelligence Center (MSTIC)
- Iranian targeting of IT sector on the rise | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit
- Exposing POLONIUM activity and infrastructure targeting Israeli organizations | Microsoft Threat Intelligence Center (MSTIC)

Schnelle Ausnutzung von Schwachstellen

Wenn Organisationen ihre Cybersicherheit stärken, reagieren nationalstaatliche Akteure mit neuen und einzigartigen Taktiken, um Angriffe auszuführen und einer Entdeckung zu entgehen. Die Identifizierung und Ausnutzung von bisher unbekannten Sicherheitslücken, die als Zero-Day-Schwachstellen bezeichnet werden, ist eine wichtige Taktik bei diesen Anstrengungen.

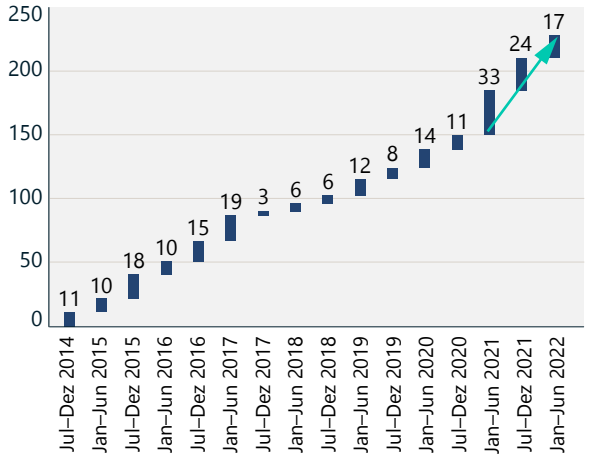
Zero-Day-Schwachstellen sind ein besonders effektives Mittel für eine erste Ausnutzung. Sobald sie öffentlich verfügbar sind, können Sicherheitslücken von anderen nationalstaatlichen und kriminellen Akteuren schnell wiederverwendet werden. Die Anzahl von öffentlich offengelegten Zero-Day-Schwachstellen entspricht dem Vorjahr mit dem bis dahin höchsten verzeichneten Wert.

Weil Cyberakteure – sowohl nationalstaatliche als auch kriminelle – immer geschickter bei der Ausnutzung dieser Schwachstellen wurden, haben wir einen Verringerung der Zeit zwischen der Bekanntgabe einer Schwachstelle und ihrer Kommerzialisierung beobachtet. Dies macht es unerlässlich, dass Organisationen Schwachstellen sofort patchen. Ebenso wichtig ist es, dass Organisationen oder Einzelpersonen, die neue Schwachstellen aufdecken, diese verantwortungsbewusst und gemäß den koordinierten Verfahrensweisen zum Offenlegen von Schwachstellen so schnell wie möglich den betroffenen Anbietern anzeigen oder melden.

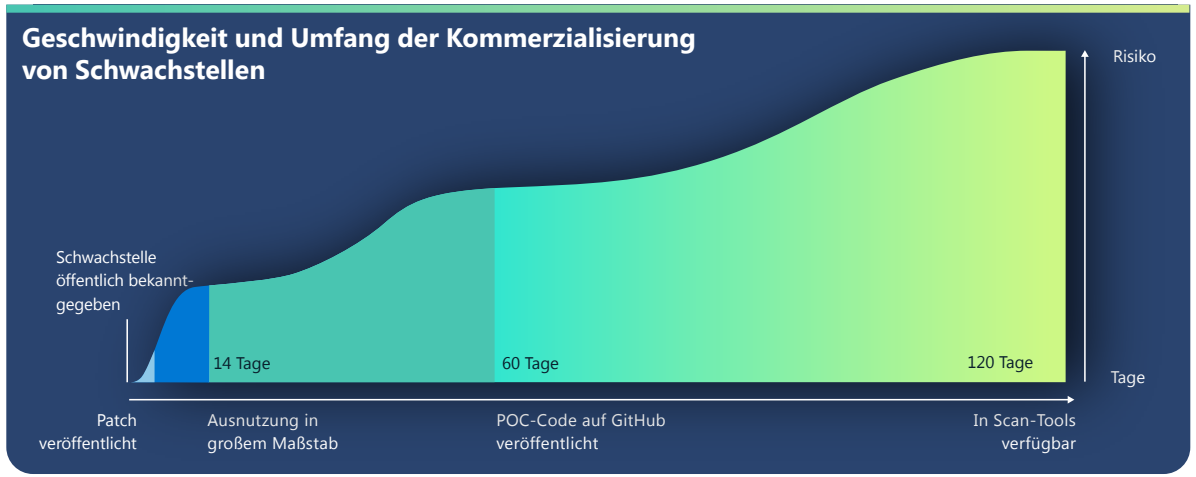
Dadurch wird sichergestellt, dass Schwachstellen identifiziert und zeitnah Patches entwickelt werden, um Kund*innen vor bisher unbekannten Bedrohungen zu schützen.

Viele Organisationen gehen davon aus, dass die Wahrscheinlichkeit, Opfer von Zero-Day-Exploit-Angriffen zu werden, geringer ist, wenn die Schwachstellenverwaltung integraler Bestandteil ihrer Netzwerksicherheit ist. Die Kommerzialisierung von Exploits führt jedoch dazu, dass diese viel häufiger auftreten. Zero-Day-Exploits werden häufig von anderen Akteuren entdeckt und in kurzer Zeit wiederverwendet. Dadurch sind ungepatchte Systeme gefährdet. Auch wenn die Ausnutzung von Zero-Day-Schwachstellen möglicherweise nur schwer zu erkennen ist, sind die Aktionen der Akteure nach dem Exploit oft leichter auszumachen. Wenn dies von vollständig gepatchter Software ausgeht, kann es zudem als ein Warnzeichen für eine Kompromittierung dienen.

Patches für Zero-Day-Schwachstellen



Anzahl öffentlich bekannter Zero-Day-Exploits aus der Liste der typischen Schwachstellen und Expositionen (CVEs).



Nach der Offenlegung einer Schwachstelle dauert es im Durchschnitt nur 14 Tage, bis ein Exploit in freier Wildbahn verfügbar ist. Diese Darstellung zeigt eine Analyse der Zeitachsen für die Ausnutzung von Zero-Day-Schwachstellen sowie die Anzahl von Systemen, die für den jeweils angegebenen Exploit anfällig sind und ab dem Zeitpunkt der ersten Veröffentlichung im Internet aktiv sind.

Auch wenn bei Angriffen auf Zero-Day-Schwachstellen anfänglich lediglich eine begrenzte Gruppe von Organisationen ins Visier genommen wird, werden sie schnell in die größere Infrastruktur der Akteure übernommen. Das ist der Startschuss für ein Rennen der Akteure, bei dem es darum geht, die Schwachstelle so weit wie möglich auszunutzen, bevor ihre möglichen Ziele Patches installieren.

Während wir viele nationalstaatliche Akteure beobachten, die Exploits aus unbekannten Schwachstellen entwickeln, sind nationalstaatliche Akteure aus China im Entdecken und Entwickeln von Zero-Day-Exploits besonders versiert. Chinas Richtlinie zum Melden von Schwachstellen trat im September 2021 in Kraft. Dies war weltweit das erste Mal, dass eine Regierung das Melden von Schwachstellen gegenüber einer Regierungsbehörde vorschrieb, damit diese die Schwachstelle prüfen kann, noch bevor sie den Besitzer*innen des Produkts oder Dienstes mitgeteilt wird. Diese neue Verordnung könnte es Beteiligten in der chinesischen Regierung ermöglichen, gemeldete Schwachstellen zu sammeln, um sie später als Waffe einzusetzen. Die verstärkte Nutzung von Zero-Day-Exploits im letzten Jahr durch chinesische Akteure bildet vermutlich das erste vollständige Jahr der landesspezifischen Vorschrift für die Schwachstellenmeldung in der chinesischen Sicherheitscommunity ab und markiert einen wichtigen Schritt für diesen Angriffstyp als staatliche Priorität. Die unten beschriebenen Schwachstellen wurden zunächst von chinesischen nationalstaatlichen Akteuren bei Angriffen entwickelt und bereitgestellt, bevor sie entdeckt und unter anderen Akteuren in der größeren Bedrohungsinfrastruktur verbreitet wurden.

Schnelle Ausnutzung von Schwachstellen

Fortsetzung

Selbst Organisationen, die kein Ziel von nationalstaatlichen Angriffen sind, bleibt nur wenig Zeit zum Patchen von Zero-Day-Schwachstellen in den betroffenen Systemen, bevor diese von der breiter gefassten Infrastruktur der Akteure ausgenutzt werden.

Diese Beispiele für neu identifizierte Schwachstellen zeigen, dass für Organisationen zwischen dem Patchen einer Schwachstelle und der Verfügbarkeit eines POC-Codes (Proof of Concept) im Durchschnitt 60 Tage liegen. Häufig wird der POC-Code dann von anderen Akteuren zur Wiederverwendung aufgegriffen. In ähnlicher Weise haben Organisationen im Durchschnitt 120 Tage Zeit, bis eine Schwachstelle in automatisierten Tools zum Scannen und Ausnutzen von Schwachstellen wie Metasploit verfügbar ist, was oft dazu führt, dass der Exploit in großem Maßstab verwendet wird. Dies weist darauf hin, dass selbst Organisationen, die kein Ziel von nationalstaatlichen Akteuren sind, nur wenig Zeit zum Patchen von Zero-Day-Schwachstellen in den betroffenen Systemen bleibt, bevor diese von der breiter gefassten Infrastruktur der Akteure ausgenutzt werden.

CVE-2021-35211 SolarWinds Serv-U

Im Juli 2021 hat SolarWinds eine Sicherheitsempfehlung für CVE -2021-35211 veröffentlicht und die Benachrichtigung Microsoft zugeschrieben.[8] Zu diesem Zeitpunkt hatten wir entdeckt, dass der mit einem Nationalstaat verbundene Akteur DEV-0322 die SolarWinds Serv-U-Schwachstelle aktiv ausnutzt. Unser RiskIQ-Team beobachtete 12.646 IP-Adressen, die zwischen dem 15. Juni und dem 9. Juli mit dem Internet verbundene Versionen der betroffenen Geräte hosteten.

CVE-2021-40539 Zoho ManageEngine ADSelfService Plus

Im September 2021 beobachteten unsere Forscher*innen mit China verbundene Akteure bei der Ausnutzung der Zoho ManageEngine bei mehreren Entitäten in den USA. Die Schwachstelle wurde am 6. September öffentlich gemeldet als CVE -2021-40539 Zoho ManageEngine ADSelfService Plus. Organisationen verwenden diesen Dienst normalerweise zum Verwalten von Kennwortrücksetzungen.[9] DEV-0322 nutzte die Schwachstelle später im September aus und setzte sie als ersten Vektor ein, um in Netzwerken Fuß zu fassen und zusätzliche Aktionen durchzuführen. Dazu gehörten etwa das Offenlegen von Anmeldeinformationen, die Installation individueller Binärdateien und das Einschleusen von Schadsoftware zum Aufrechterhalten der Persistenz. Zum Zeitpunkt der Offenlegung beobachtete RiskIQ 4.011 Instanzen dieser Systeme aktiv und im Internet.

CVE-2021-44077 Zoho ManageEngine ServiceDesk Plus

Ende Oktober 2021 beobachteten wir DEV-0322 bei der Ausnutzung einer Schwachstelle (CVE -2021-44077) in einem zweiten Zoho ManageEngine-Produkt: Servicedesk Plus. Dabei handelt es sich um eine Software mit Ressourcenverwaltung für IT-Helpdesks. DEV-0322 nutzte diese Schwachstelle zum Angreifen und Kompromittieren von Entitäten im Gesundheitswesen, in der IT, in Hochschulen und in kritischer Infrastruktur. Am 2. Dezember gaben das Federal Bureau of Investigation (FBI) und die Cybersecurity and Infrastructure Security Agency (KAG) eine gemeinsame Warnung für die Öffentlichkeit heraus, bei der es um die Ausnutzung dieser Schwachstelle durch nationalstaatliche Akteure ging. Zum Zeitpunkt der Offenlegung beobachtete RiskIQ 7.956 Instanzen dieser Systeme aktiv und im Internet.

CVE-2021-42321 Microsoft Exchange

Ein Zero-Day-Exploit für eine Exchange-Schwachstelle, CVE-2021-42321, wurde während des Tianfu Cup enthüllt, eines internationalen Cybersicherheitsgipfels und Hackerwettbewerbs, der am 16. und 17. Oktober 2021 in Chengdu, China, stattfand. Sicherheitsforscher*innen bei Microsoft beobachteten den Exploit für die Exchange-Schwachstelle, die am 21. Oktober in freier Wildbahn verwendet wurde, nur drei Tage nach Aufdeckung der Schwachstelle. Zum Zeitpunkt der Offenlegung beobachtete RiskIQ 61.559 Instanzen dieser Systeme aktiv und im Internet. Wir haben die Ausnutzung der Schwachstelle bis in den November 2021 beobachtet.

CVE-2022-26134 Confluence

Ein mit China verbundener Akteur war vermutlich vier Tage vor ihrer öffentlichen Bekanntgabe am 2. Juni im Besitz des Zero-Day-Codes für die Confluence-Schwachstelle (CVE -2022-26134) und setzte ihn wahrscheinlich gegen eine Entität in den USA ein. Zum Zeitpunkt der Offenlegung beobachtete RiskIQ 53.621 Instanzen vulnerabler Confluence-Systeme im Internet.

Das Aufgreifen und die Ausnutzung von Schwachstellen erfolgen in großem Maßstab und in immer kürzeren Zeitabständen.

Umsetzbare Insights

1. Priorisieren Sie das Patchen von Zero-Day-Schwachstellen, sobald diese veröffentlicht werden. Warten Sie nicht, bis die Bereitstellung über den Zyklus der Patchverwaltung erledigt wird.
2. Dokumentieren und inventarisieren Sie alle Hardware- und Softwareressourcen des Unternehmens, um Risiken zu ermitteln und schnell zu bestimmen, wann Patches erforderlich sind.

Cybertaktiken russischer Akteure zu Kriegszeiten bedrohen die Ukraine und andere Länder

In diesem Jahr begannen staatliche russische Akteure Cyberoperationen, um die militärischen Maßnahmen bei Russlands Angriffskrieg gegen die Ukraine zu flankieren. Häufig wandten sie dabei die gleichen Taktiken und Techniken an, die auch gegen Ziele außerhalb der Ukraine eingesetzt wurden. Es ist von entscheidender Bedeutung, dass Unternehmen weltweit Maßnahmen ergreifen, um die Cybersicherheit gegen digitale Bedrohungen von mit Russland verbundenen Akteuren zu stärken.

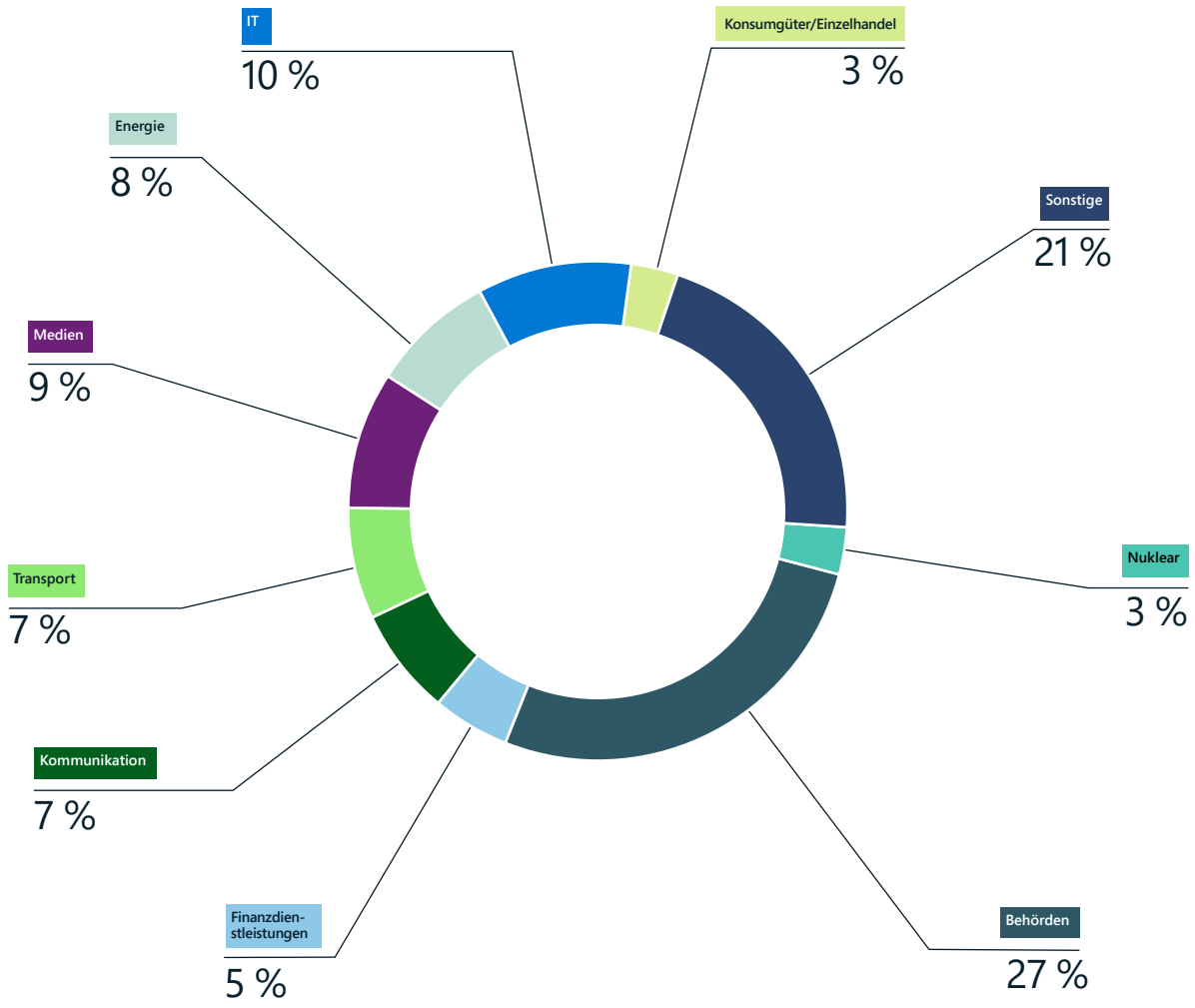
Die Situation vor Ort schwankt weiterhin, weil der militärische Konflikt anhält, und die Ukraine und ihre Verbündeten sollten bereit sein, sich zu verteidigen, wenn staatliche russische Cyberakteure die Häufigkeit oder Intensität von Angriffen im Gleichklang mit den militärischen Zielen erhöhen. In den ersten vier Monaten des Krieges hat Microsoft beobachtet, wie Akteure, die mit dem russischen Militär zusammenhängen, mehrere Wellen zerstörerischer Cyberangriffe gegen fast 50 verschiedene ukrainische Behörden und Unternehmen sowie auf Spionage abzielende Angriffe gegen viele weitere durchführten. Aktionen gegen Kund*innen von Onlinediensten nicht mitgezählt, richteten sich zwischen Ende Februar und Juni 64 % der russischen Aktivitäten, bei denen die Ziele bekannt waren, gegen Organisationen in der Ukraine.

Bei jeder Operation setzten russische Akteure viele der Taktiken, Techniken und Verfahren (Tactics, Techniques and Procedures, TTPs) ein, deren Nutzung gegen Ziele innerhalb und außerhalb der Ukraine wir schon vor Kriegsbeginn beobachtet hatten. Diese Akteure hatten in der ersten Phase des Konflikts die Absicht, Daten zu vernichten und ukrainische Regierungsbehörden zu destabilisieren. Seither haben sie versucht, den Transport von militärischer und humanitärer Hilfe in die Ukraine zu behindern, den öffentlichen Zugang zu Dienstleistungen und Medien zu stören und Informationen von längerfristigem nachrichtendienstlichen oder wirtschaftlichen Nutzen für Russland zu stehlen.

Angriffe auf das Transportwesen bedrohen einen Bereich von entscheidender Bedeutung für ukrainische Bürger*innen, die versuchen, den Konflikt zu überleben. Laut einer von UNICEF in Auftrag gegebenen Umfrage im Mai machten sich die Befragten in vom Konflikt betroffenen städtischen Gebieten die meisten Sorgen über das Transportwesen und Lieferengpässe bei der Kraftstoffversorgung sowie über die Sicherheit und Einschränkungen beim Zugang zu Lebensmitteln, medizinischen Dienstleistungen und Finanzdienstleistungen.[10] Im Juni sagte der UNO-Krisenkoordinator für die Ukraine, dass mindestens 15,7 Millionen Menschen in der Ukraine dringend humanitäre Hilfe benötigten. Bei einem Andauern des Krieges werde die Zahl noch weiter ansteigen.[11]

Außerhalb der Ukraine verzeichnete Microsoft zwischen Ende Februar und Juni russische Eindringversuche in Netzwerke von 128 Organisationen in 42 Ländern. Die USA waren das vorrangige Ziel von Russland. Polen, ein Transitland für einen Großteil der internationalen und militärischen Hilfe für die Ukraine, war während dieses Zeitraums ebenfalls ein wichtiges Ziel. Im April und im Mai haben mit dem russischen Staat verbundene Akteure Organisationen in den baltischen Staaten und Computernetzwerke in Dänemark, Norwegen, Finnland und Schweden verfolgt.

Die am häufigsten angegriffenen Industriezweige in der Ukraine seit Kriegsbeginn



Während des gesamten Konflikts sind staatliche Organisationen auf kommunaler, bundesstaatlicher und föderaler Ebene ein vorrangiges Ziel für staatliche und staatsnahe russische Gruppen geblieben. Der Schwerpunkt auf Transport-, Energie-, Finanz- und Medienunternehmen unterstreicht das Risiko, das diese Cyberoperationen für Dienstleistungen darstellen, von denen die ukrainischen Bürger*innen abhängen.

Cybertaktiken russischer Akteure zu Kriegszeiten bedrohen die Ukraine und andere Länder

Fortsetzung

Wir haben eine Zunahme ähnlicher Aktivitäten festgestellt, die sich gegen die Außenministerien von NATO-Staaten richteten.

Staatliche russische Gruppen waren im vergangenen Jahr weiterhin daran interessiert, die kritische Infrastruktur innerhalb und außerhalb der Ukraine zu kompromittieren. IRIDIUM hat die Industroyer2-Schadsoftware bei einem gescheiterten Versuch eingesetzt, Millionen von Menschen in der Ukraine von der Stromversorgung abzuschneiden. Anfang 2022 führte BROM außerhalb der Ukraine Eindringversuche gegen Unternehmen durch, die in der Fertigung und bei industriellen Steuerungssystemen tätig waren.

Staatliche und staatsnahe russische Akteure haben in diesem Jahr Cyberoperationen gegen die Ukraine, deren Verbündete und weitere Ziele von nachrichtendienstlichem Wert durchgeführt. Dabei kamen viele der folgenden TTPs zum Einsatz:

Spear-Phishing mit bösartigen Anhängen oder Links

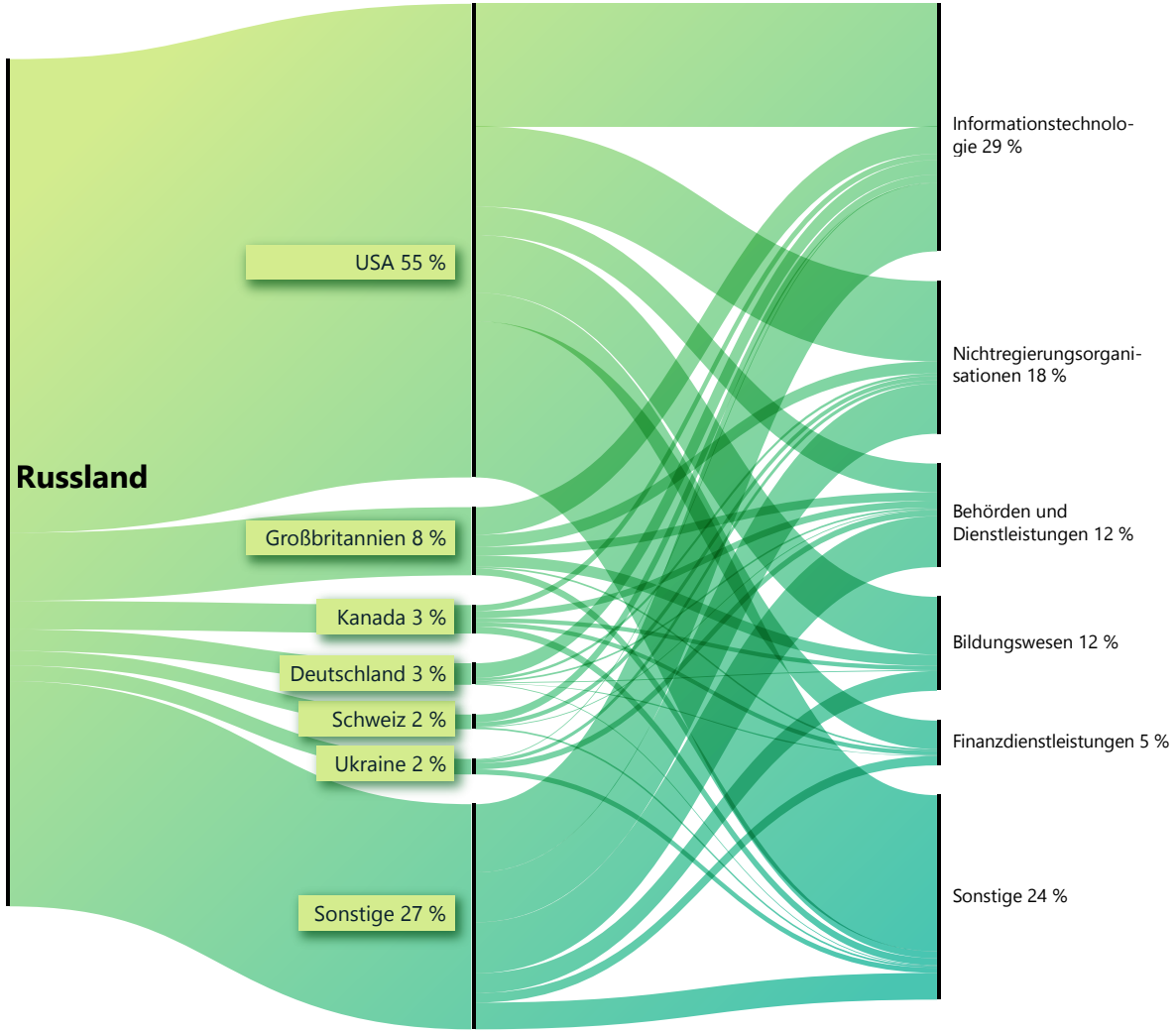
Staatliche und staatsnahe russische Gruppen wie ACTINIUM, NOBELIUM, STRONTIUM, DEV-0257, SEABORGIUM und IRIDIUM setzten allesamt Phishing-Kampagnen ein, um einen ersten Zugriff auf die gewünschten Konten und Netzwerke in Organisationen innerhalb und außerhalb der Ukraine zu erhalten. Viele Kampagnen nutzten kompromittierte oder gefälschte Konten bei Zielorganisationen oder innerhalb derselben Branche sowie überzeugende Themen, um die Opfer zu ködern. NOBELIUM setzte kompromittierte diplomatische Konten ein, um Phishing-Mails zu versenden, die als diplomatische Kommunikation an Mitarbeiter*innen von Außenministerien auf der ganzen Welt getarnt waren. STRONTIUM erstellte Spoofing-Konten anhand öffentlich verfügbarer Namen von Kontoinhaber*innen bei Thinktanks in den USA und versendete Phishing-E-Mails, um Zugriff auf Konten bei diesen Thinktanks zu erbeuten. SEABORGIUM führte Phishing-Kampagnen mit Ködern durch, die sich auf die Berichterstattung über den Konflikt in der Ukraine bezogen, um ersten Zugriff auf Konten bei Thinktanks in den nördlichen Ländern zu erhalten, die sich mit internationalen Angelegenheiten befassen.

Ausnutzung der IT-Services-Lieferkette, um nachgelagerte Kund*innen zu beeinflussen

Ende 2021 haben staatliche russische Akteure IT-Dienstanbieter kompromittiert und den Zugriff für die Manipulation von Websites und die Einschleusung der destruktiven Whispergate-Schadsoftware durch DEV-0586 im Januar genutzt.[12] DEV-0586 kompromittierte außerdem das Netzwerk eines IT-Unternehmens, das Ressourcenverwaltungssysteme für das ukrainische Verteidigungsministerium und andere Organisationen im Kommunikations- und Transportsektor entwickelt hat. Das deutet darauf hin, dass die Gruppe auch Angriffsoptionen auf Dritte in diesen Sektoren auslotete.

Weltweit, aber vor allem in den USA und Westeuropa, griff NOBELIUM Anbieter von IT-Dienstleistungen an, um im ganzen Zeitraum von 2021 bis 2022 Zugriff auf staatliche Einrichtungen und weitere sensible Netzwerke zu erlangen (siehe die Erörterung der Schwachstellen in der Lieferkette weiter oben in diesem Kapitel).

Russland: Die am häufigsten angegriffenen Länder und Industriezweige



Auch wenn sich der Fokus auf Organisationen in der Ukraine seit Anfang 2022 verstärkte, richteten sich die meisten Angriffe nach wie vor gegen Kund*innen von Onlinediensten in Nordamerika und Westeuropa. Die Kampagne von NOBELIUM gegen den IT-Sektor hat diesen zum am häufigsten angegriffenen Sektor des vergangenen Jahres gemacht.

Cybertaktiken russischer Akteure zu Kriegszeiten bedrohen die Ukraine und andere Länder

Fortsetzung

Ausnutzung öffentlich zugänglicher Anwendungen, um ersten Zugriff auf Netzwerke zu erhalten

Seit mindestens Ende 2021 hat STRONTIUM seine Fähigkeiten beim Ausnutzen öffentlich zugänglicher Dienste wie Microsoft Exchange Server zum Stehlen von Informationen entwickelt und ausgebaut. STRONTIUM hat ungepatchte Exchange Server ausgenutzt, um Zugriff auf ukrainische Regierungskonten sowie auf Organisationen im Militär- und Rüstungsbereich in den USA, dem Libanon, Peru und Rumänien zu erlangen sowie auf weitere Regierungsbehörden in Armenien, Bosnien, dem Kosovo und Malaysia. DEV-0586 wird auch mit dem russischen Militär in Verbindung gebracht und hat die Schwachstellen von Confluence-Servern ausgenutzt, um ersten Zugriff auf Organisationen von staatlichen Stellen und im IT-Sektor in der Ukraine und anderen osteuropäischen Ländern zu erhalten.

Staatliche und staatsnahe russische Akteure nutzen viele der gleichen TTPs, um Organisationen von Interesse in Kriegs- und Friedenszeiten zu kompromittieren.

Verwendung von administrativen Konten und Protokollen sowie native Dienstprogramme für die Netzwerkermittlung und laterale Bewegung

Microsoft hat beobachtet, wie staatliche russische Akteure nach dem ersten Zugriff auf ein Netzwerk über legitime Konten und Software-Dienstprogramme grundlegende Wartungsaufgaben durchführten, um eine Entdeckung so lange wie möglich hinauszuzögern. Sie stützten sich dabei auf kompromittierte Identitäten mit administrativen Funktionen und gültigen Verwaltungsprotokollen sowie auf Tools und Methoden, um sich innerhalb von Netzwerken lateral zu bewegen, ohne sofort die Aufmerksamkeit von automatisierten Monitoren und Netzwerkverteidigern zu erregen.

Grundlegende Cyberhygiene und die Anwendung von Tools für Erkennung und Reaktion am Endpunkt können dazu beitragen, die negativen Auswirkungen von Operationen dieser Art sowohl in Friedenszeiten sowie auch zu Kriegszeiten abzumildern.

Die Unvorhersehbarkeit des anhaltenden Konflikts erfordert, dass Unternehmen weltweit Maßnahmen ergreifen, um die Cybersicherheit im Hinblick auf digitale Bedrohungen von staatlichen und staatsnahen russischen Akteuren zu erhöhen.

Umsetzbare Insights

1. Minimieren Sie den Diebstahl von Anmeldeinformationen und den Missbrauch von Konten, indem Sie die Identitäten Ihrer Benutzer*innen durch das Implementieren von MFA-Tools zum Identitätsschutz und das Erzwingen von Zugriff mit den geringstmöglichen Berechtigungen schützen, um die sensibelsten und privilegiertesten Konten und Systeme abzusichern.
2. Führen Sie Aktualisierungen durch, um sicherzustellen, dass all Ihre Systeme so schnell wie möglich das höchste Schutzniveau erreichen und auf dem neuesten Stand bleiben.
3. Stellen Sie in Ihrem ganzen Unternehmen Antischadsoftware sowie Lösungen für Erkennung am Endpunkt und Identitätsschutz bereit. Eine Kombination aus tiefgreifenden Sicherheitslösungen auf der einen und geschulten und kompetenten Mitarbeiter*innen auf der anderen Seite kann Ihre Organisation befähigen, Angriffe mit Auswirkungen auf Ihre Geschäftstätigkeit zu identifizieren, aufzuspüren und zu verhindern.
4. Ermöglichen Sie Untersuchungen und Wiederherstellung für den Fall, dass Sie eine Bedrohung für Ihre Umgebung ermitteln oder erhalten. Sichern Sie dazu kritische Systeme, und aktivieren Sie die Protokollierung. Die Einrichtung eines Reaktionsplans für Vorfälle (Incident Response Plan) wird dringend empfohlen.

Links zu weiteren Informationen

- Defending Ukraine: Early Lessons from the Cyber War | Microsoft On the Issues
- The hybrid war in Ukraine | Microsoft On the Issues
- Cyber threat activity in Ukraine: analysis and resources | Microsoft Security Response Center (MSRC)
- Disrupting cyberattacks targeting Ukraine | Microsoft On the Issues
- Malware attacks targeting Ukraine government | Microsoft On the Issues
- MagicWeb: NOBELIUM's post-compromise trick to authenticate as anyone | Microsoft Threat Intelligence Center (MSTIC), Detection and Response Team (DART), Microsoft 365 Defender Research Team

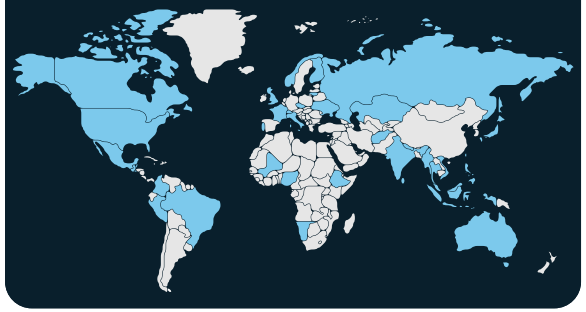
China steigert weltweite Angriffe zur Erlangung von Wettbewerbsvorteilen

Im komplexen geopolitischen Klima von heute führen staatliche und staatsnahe chinesische Akteure Cyberoperationen häufig mit dem Ziel durch, die strategischen militärischen und wirtschaftlichen Ziele des Landes sowie die Ziele in Bezug auf die auswärtigen Beziehungen voranzutreiben. All dies ist Teil von Chinas Bestrebungen, sich einen Wettbewerbsvorteil zu verschaffen. Im letzten Jahr hat Microsoft weit verbreitete chinesische Aktivitäten gegen Länder auf der ganzen Welt beobachtet.

Seit Mitte 2021 versuchte China, inmitten des schlimmsten Anstiegs von COVID-19 der letzten beiden Jahre durch verschiedene Manöver wirtschaftliche und finanzielle Stabilität sicherzustellen.[13] China jonglierte weiterhin mit seiner Haltung zu geopolitischen Ereignissen, etwa das Bemühen um einen ausgewogenen Standpunkt in seiner „grenzenlosen" Partnerschaft mit Russland,[14] um seine Position auf der Weltbühne zu sichern.[15] Darüber hinaus strapazierte Chinas Haltung gegenüber den USA und ihren Verbündeten in Bezug auf Taiwan[16] und das südchinesische Meer nach wie vor die Außenbeziehungen zu vielen Ländern.[17]

Staatliche und staatsnahe chinesische Gruppen weiteten Angriffe gegen kleinere Nationen auf der ganzen Welt aus. Ein Fokus lag dabei auf Südostasien, um auf sämtlichen Fronten Wettbewerbsvorteile zu gewinnen.

Von staatlichen und staatsnahen chinesischen Gruppen anvisierte Länder

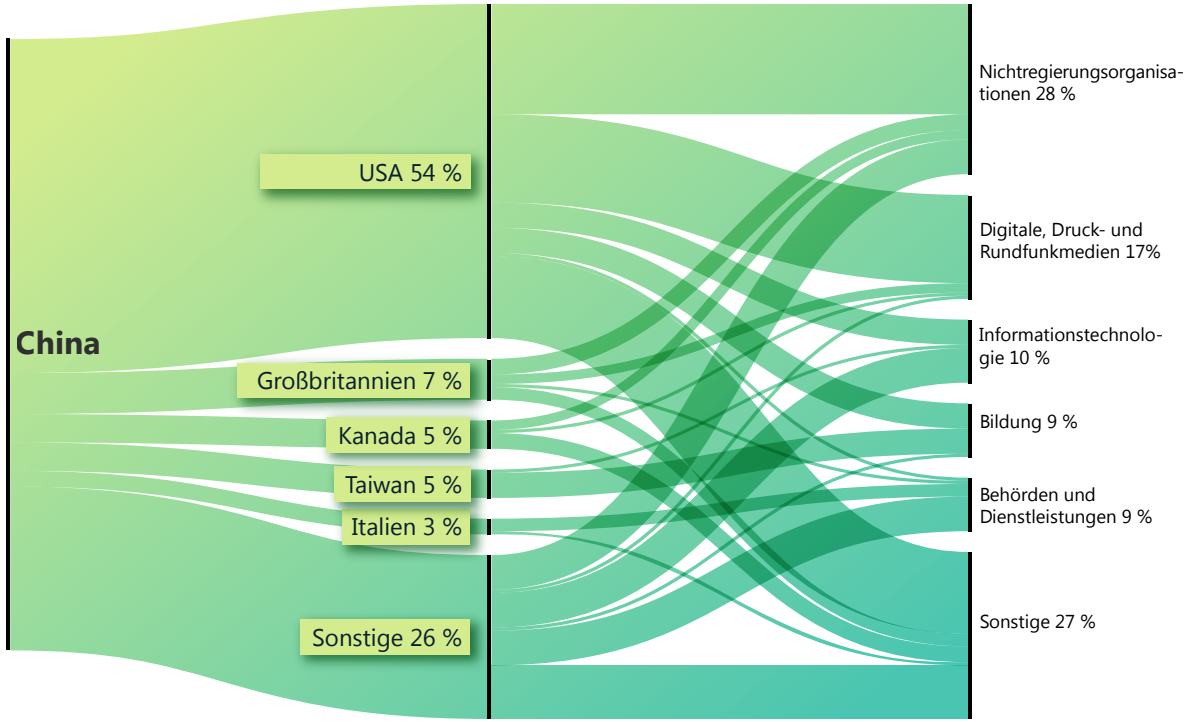


China hat seinen wirtschaftlichen Einfluss weltweit auch durch zuvor etablierte Belt-and-Road-Initiativen (BRI) erweitert. Dabei ging es um den Versuch, einen umfassenden Investitionsrahmen mit der EU[18] zu befördern und neue regionale Handelsabkommen mit 15 Ländern im asiatisch-pazifischen Raum auszuhandeln, die sogenannte Regional Comprehensive Economic Partnership.[19] Aufgrund der beobachteten Cyberoperationen und der Bandbreite der angegriffenen Ziele geht Microsoft davon aus, dass China kollektive Cyberangriffe weiterhin als Instrument nutzen wird, um seine strategischen politischen, militärischen und wirtschaftlichen Ziele weiter voranzutreiben.

Cyberangriffe werden wahrscheinlich für das Vorantreiben wirtschaftlicher und militärischer Interessen eingesetzt.

Microsoft hat weitverbreitete Angriffe von staatlichen und staatsnahen chinesischen Gruppen gegen kleinere Nationen auf der ganzen Welt beobachtet. Dies deutet darauf hin, dass China Cyberspionage wahrscheinlich als eine Komponente seines weltweiten wirtschaftlichen und militärischen Einflusses einsetzt.

China: Die am häufigsten angegriffenen Länder und Industriezweige



Thinktanks/NGOs, Medien, IT, staatliche Einrichtungen und das Bildungswesen gehörten zu den am häufigsten angegriffenen Sektoren von in China ansässigen Gruppen, wahrscheinlich zur persistenten Aufklärung und Informationsgewinnung.

Die Spanne der Ziele umfasste unter anderem Länder in Afrika, der Karibik, dem Nahen Osten, Ozeanien und Südasien. Dabei lag der Fokus insbesondere auf Ländern in Südostasien und den Pazifischen Inseln.

Im Einklang mit der BRI-Strategie Chinas haben die in China ansässigen Gruppen Entitäten in Afghanistan, Kasachstan, Mauritius, Namibia und Trinidad und Tobago ins Ziel genommen.[20] So war Trinidad und Tobago beispielsweise das erste karibische Land, das die BRI-Strategie Chinas 2018 unterstützte, und China hält es für einen wichtigen Partner in der Region. NICKEL hat seit 2021 persistente Netzwerkaktivitäten gegen Trinidad und Tobago durchgeführt. Im März 2022 führte NICKEL beispielsweise Aufklärungsaktivitäten durch, die eine Regierungsbehörde anvisierten, um Informationen zu sammeln.

China steigert weltweite Angriffe zur Erlangung von Wettbewerbsvorteilen

Fortsetzung

In der Zwischenzeit hat Microsoft beobachtet, dass staatliche und staatsnahe chinesische Gruppen ihre Netzwerkoperationen auf Entitäten in Südostasien konzentrierten und auf die Länder der Pazifischen Inseln ausdehnten, weil China seine militärischen und wirtschaftlichen Prioritäten verlagerte, um den Herausforderungen durch die neuerlichen Interessen der USA in der Region zu begegnen. Im Januar 2022 beobachtete Microsoft, wie RADIUM ein Energieunternehmen und eine mit Energiefragen zusammenhängende Regierungsbehörde in Vietnam sowie eine indonesische Regierungsbehörde angriff. Die Aktivitäten von RADIUM stellen wahrscheinlich auf die strategischen Ziele Chinas im Südchinesischen Meer ab.[21] Ende Februar und Anfang März kompromittierte GALLIUM mehr als 100 Konten, die mit einer prominenten internationalen Organisation (Intergovernmental Organization, IGO) in der südostasiatischen Region zusammenhängen. GALLIUMs Angriff auf die IGO in der Region erfolgte zeitgleich mit der Ankündigung eines geplanten Treffens zwischen den USA und führenden Landesvertreter*innen. Die GALLIUM-Akteure hatten wahrscheinlich den Auftrag, die Kommunikation vor diesem Ereignis zu überwachen und Erkenntnisse zu sammeln.

Weil China seinen Einfluss in Ländern der Pazifischen Inseln ausdehnte, folgten Aktivitäten chinesischer Gruppen. Im April unterzeichneten China und die Salomonen ein Sicherheitsabkommen, das „Frieden und Sicherheit fördern“ soll. Mit diesem Abkommen kann China potenziell bewaffnete Polizei- und Militärkräfte auf den Salomoninseln stationieren.[22] Im Mai war China Gastgeber des zweiten Außenministertreffens zwischen China und den Ländern der Pazifischen Inseln auf Fidschi und schlug vor, eine „umfangreiche strategische Partnerschaft“ voranzutreiben, um die politischen, kulturellen, sozialen Interessen sowie auch die Interessen in puncto Sicherheit und Klimawandel zu fördern und außerdem die Pandemie zu bekämpfen.[23] Etwa zur gleichen Zeit identifizierte Microsoft die Schadsoftware von GADOLINIUM auf den Regierungssystemen der Salomonen. Außerdem führte RADIUM bösartigen Code auf den Systemen eines Telekommunikationsunternehmens in Papua-Neuguinea aus. Unserer Einschätzung nach dienten diese Aktivitäten wahrscheinlich dem Sammeln von Informationen, um Chinas regionale Gesamtstrategie zu unterstützen.

Microsoft unterbindet Aktivitäten von NICKEL, doch die Gruppe zeigt ihre Hartnäckigkeit.

Im Dezember 2021 reichte die Microsoft Digital Crimes Unit (DCU) Schriftsätze beim US-Bezirksgericht für den Eastern District of Virginia ein, um die Erlaubnis zu erhalten, 42 Command-and-Control-Domänen (C2) zu beschlagnahmen, die von NICKEL kontrolliert wurden. Diese C2-Domänen wurden seit September 2019 gegen Regierungen, diplomatische Organisationen und NGOs in Mittel- und Südamerika, der Karibik, Europa und Nordamerika eingesetzt.[24] Bei diesen Operationen erreichte NICKEL langfristigen Zugriff auf mehrere Entitäten und exfiltrierte seit Ende 2019 beständig Daten von einigen Opfern.

Weil China damit fortfährt, bilaterale Wirtschaftsbeziehungen mit weiteren Ländern zu etablieren – häufig in Abkommen, die mit der BRI assoziiert sind –, wird der weltweite Einfluss von China weiter zunehmen. Wir gehen davon aus, dass staatliche und staatsnahe chinesische Akteure Ziele in ihren staatlichen Einrichtungen und den diplomatischen und NGO-Sektoren verfolgen werden, um neue Insights zu erhalten, mit denen sie wahrscheinlich Wirtschaftsspionage oder herkömmliche Informationssammlung betreiben wollen. Seit der Stilllegung durch Microsoft hat NICKEL mehrere Regierungsbehörden angegriffen – vermutlich in dem Versuch, den Zugriff zurückzuerlangen. Zwischen Ende März und Mai 2022 hat NICKEL mindestens fünf Regierungsbehörden auf der ganzen Welt erneut kompromittiert. Dies deutet darauf hin, dass die Gruppe über zusätzliche Einstiegspunkte für diese Entitäten verfügt oder erneut Zugriff über neue C2-Domänen erlangt hat. Die Beharrlichkeit von NICKEL bei der wiederholten Kompromittierung derselben weltweiten Behörden deutet darauf hin, wie wichtig diese Aufgabe auf hoher Ebene ist.

China tritt außenpolitisch energischer auf. Wir gehen davon aus, dass auch die cybergestützte Wirtschaftsspionage und Informationssammlung weitergehen werden.

Umsetzbare Insights

1. Stärken Sie die Cyberabwehr zur proaktiven Abschwächung von Cyberbedrohungen. Die Hartnäckigkeit chinesischer Akteure verlangt von Unternehmen, mögliche Angriffe rechtzeitig zu identifizieren, zu erkennen, sich davor zu schützen und darauf zu reagieren.
2. Akteure missbrauchen geplante Aufgaben[25] als gängige Methode zum Erreichen von Persistenz und Umgehen von Verteidigungsmaßnahmen. Sorgen Sie dafür, dass Ihre Umgebung ausreichend Sicherheitsrichtlinien implementiert, um gegen diese häufig eingesetzte Technik geschützt zu sein.[26]
3. Wir beobachten außerdem die Verwendung von Web-Shells als ersten Vektor beim Eindringen in anvisierte Netzwerke.[27] Organisationen sollten ihre Systeme gegen Web-Shells-Angriffe stärken, über die Angreifer Zugriff für das Ausführen von Remote-Befehlen erhalten können.[28]

Links zu weiteren Informationen

- NICKEL targeting government organizations across Latin America and Europe | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit (DSU)
- Protecting people from recent cyberattacks | Microsoft On the Issues

Iran wird nach dem Machtwechsel zunehmend aggressiv

Microsoft hat beobachtet, wie staatliche iranische Gruppen und damit verbundene Akteure Tempo und Umfang der Cyberangriffe gegen Israel erhöhten, Ransomware-Angriffe über regionale Gegner hinaus auf Opfer in den USA und in der EU erweiterten und kritische US-Infrastruktur anvisierten, zumindest als Vorstufe für potenziell zerstörerische Cyberangriffe.

Die zunehmende Aggression der staatlichen iranischen Akteure im Cyberspace erfolgte im Nachgang des Wechsels der Präsidentschaft. Im Sommer 2021 ersetzte der Hardliner Ibrahim Raisi den moderaten Präsidenten Hassan Rouhani. Im krassen Gegensatz zu Raisi, der ein Schützling des Obersten Führers und ein enger Verbündeter der Revolutionsgarden (Islamic Revolutionary Guard Corps, IRGC) ist, brachte die Vorliebe für Diplomatie des früheren Präsidenten Rouhani diesen häufig in Konflikt mit dem Obersten Führer und den Kommandeuren der Revolutionsgarden.[29] Die aggressiven Ansichten der Raisi-Administration scheinen die Bereitschaft der iranischen Akteure gesteigert zu haben, aggressiver gegen Israel und den Westen, insbesondere die USA, vorzugehen. Dies steht im Gegensatz zur Wiederaufnahme diplomatischer Bemühungen zur Wiederbelebung des Atomabkommens mit dem Iran.

Mehr Tempo und Umfang der iranischen Cyberattacken gegen Israel

Innerhalb weniger Wochen, nachdem Raisi die Aufstellung seines außenpolitischen Teams abgeschlossen hatte,[30] nahmen staatliche iranische Akteure die destruktiven Cyberangriffe gegen Israel wieder auf, und das mit einer höheren Schlagzahl als im Vorjahr. Diese Ransomware- und Hack-and-Leak-Angriffe wurden ab September alle paar Wochen durchgeführt, und mindestens drei mit dem Iran verbundene Akteure waren daran beteiligt. Das legt nahe, dass die Angriffe Teil einer landesweiten Vergeltungskampagne gegen Israel gewesen sein könnten. In mindestens einem Fall befand Microsoft, dass ein Ransomware-Angriff gegen eine israelische Organisation Ende 2021 einen darunter liegenden Angriff zum Löschen von Daten verschleiern sollte. Die Schadsoftwareanalyse von Microsoft zeigte, dass die beim Opfer eingeschleuste Ransomware soprogrammiert war, dass nach der Verschlüsselung eine Wiper-Schadsoftware ausgeführt wird.

Bis 2022 sind die iranischen Cyberangriffe eskaliert – sowohl bei Auswahl der Ziele als auch bei der Form der Angriffe. Im Februar versuchte DEV-0198 einen zerstörerischen Angriff auf kritische israelische Infrastruktur durchzuführen. Microsoft geht auch davon aus, dass ein mit dem Iran verbundener Akteur wahrscheinlich für einen ausgeklügelten Cyberangriff verantwortlich war, der im Juni die Alarmsirenen für einen Raketenangriff auslöste. Dabei kam vermutlich eine Software zum Einsatz, die Audio über IP-Netzwerke einregelt.

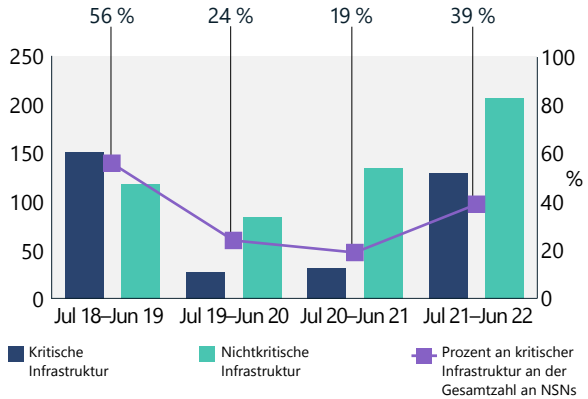
Die iranische Bedrohung für kritische US-amerikanische und israelische Infrastruktur ist über das ganze Jahr hinweg gestiegen

Nach Einschätzung von Microsoft stehen die staatlichen iranischen Akteure in Verbindung mit den iranischen Revolutionsgarden (PHOSPHOR und DEV-0198) und griffen von Ende 2021 bis Mitte 2022 prominente kritische Infrastruktur in den USA und in Israel an. Das wahrscheinliche Ziel bestand darin, Teheran Vergeltungsoptionen gegen dieselben Sektoren zu eröffnen, bei denen die Kommandeure der Revolutionsgarden die USA und Israel beschuldigten, sie im Iran gestört zu haben.[31] Wir gehen davon aus, dass diese Aktivität mit Aussagen zusammenhängt, die General Gholamreza Jalali von den Revolutionsgarden, Leiter der passiven Verteidigungsorganisation des Iran, Ende 2021 getätigt hat. Dabei wiederholte er Anschuldigungen von anderen einflussreichen Persönlichkeiten des Regimes, nach denen die USA und Israel Cyberangriffe auf iranische Häfen, Eisenbahnen und Tankstellen durchgeführt hätten.[32] Jalali verbreitete diese Anschuldigungen ein zweites Mal mit vorbereiteten Bemerkungen bei einer inszenierten Rede zum Freitagsgebet. Dabei stand er auf einem Podium mit einem Bild einer Rakete und dem Wort „USA" darauf. Das lässt vermuten, dass seine Vorgesetzten dieselbe Ansicht vertreten.[33]

PHOSPHOR begann im Oktober 2021 mit der großangelegten Auslotung von US-Organisationen nach ungepatchten Fortinet- und ProxyShell-Schwachstellen. Nach der Kompromittierung wurden über diese ungepatchten Systeme Ransomware-Angriffe durchgeführt. In vielen Fällen richteten sich diese gegen kritische Infrastruktur in den USA und weiteren westlichen Ländern. Diese markierten die ersten bestätigten Fälle von staatsnahen iranischen Ransomware-Angriffen außerhalb des Nahen Ostens. Nach dem Cyberangriff gegen iranische Tankstellen Ende Oktober beobachtete Microsoft einen Anstieg der iranischen Ransomware-Angriffe auf US-Unternehmen, was auf eine mögliche Korrelation hindeutet.

Gleichzeitig ging PHOSPHOR zu direkten Angriffen auf prominente kritische Infrastruktur in den USA über, einschließlich großer Seehäfen und Flughäfen, Schienenverkehrssystemen, Versorgungsbetrieben sowie Öl- und Gasunternehmen. Bei diesen Angriffen wurde häufig Spear-Phishing verwendet. Diese Angriffe dauerten bis Mitte 2022 an. Die Ziele entsprechen direkt den Sektoren, bei denen Teheran die USA und Israel beschuldigt, sie im Iran angegriffen zu haben, und haben Iran vermutlich Vergeltungsoptionen in die Hand gegeben. Die Kompromittierung nahezu identischer Ziele böte eine Gelegenheit zur Abschreckung zukünftiger Angriffe. Gleichzeitig zielte es auf die Vermeidung einer Eskalation ab, indem es den Grund für die Angriffe signalisierte, ohne eine Schuld einzuräumen.

Wiederaufleben der iranischen Angriffe auf Infrastruktur



Die iranischen Angriffe auf kritische Infrastruktur sind auf dem höchsten Stand, der von Ende 2018 bis Anfang 2019 beobachtet wurde. Bei der Bestimmung, ob ein Unternehmen den Kriterien für kritische Infrastruktur entspricht, haben wir die US Presidential Policy Directive 21 (PPD-21) zugrunde gelegt (Juli 2021 – Juni 2022).

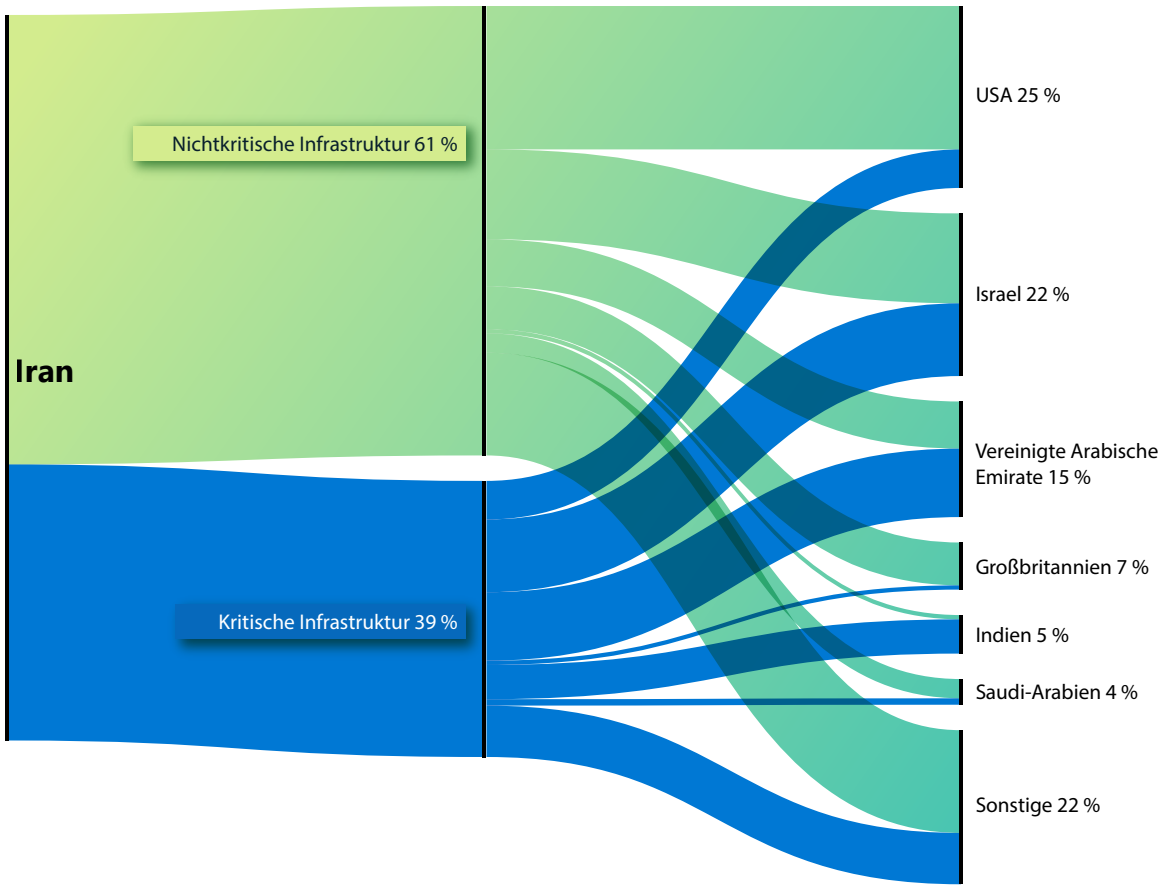
Iran wird nach dem Machtwechsel zunehmend aggressiv

Fortsetzung

In Israel nahm DEV-0198 israelische Eisenbahninfrastruktur, Logistikunternehmen, Softwareanbieter für Logistikunternehmen und Mineralölunternehmen mit einem Schwerpunkt auf Tankstellen ins Visier. Anfang 2022 führte die Gruppe einen zerstörerischen Angriff auf das Netzwerk eines großen israelischen Logistikunternehmens durch, der das Unternehmen zwang, seine Computer abzuschalten und einige seiner Abläufe herunterzufahren, um den Angriff einzudämmen. In einem anderen Fall haben wir beobachtet, wie die Gruppe versuchte, über gestohlene oder wiederverendete Anmeldeinformationen auf das Netzwerk eines großen israelischen Transportanbieters zuzugreifen. In der Zwischenzeit kompromittierte ein anderer iranischer Akteur, DEV-0343 – dessen Angriffe auf Rüstungs-, Seefracht- und Satellitenbildgebungsunternehmen Verbindungen zu den Revolutionsgarden nahelegen –, Anfang 2021 Konten bei israelischen Entitäten im Zusammenhang mit dem Transport- und Hafenwesen.

Iranische Gruppen werden wahrscheinlich eine Bedrohung für die US-amerikanischen und israelischen Verkehrs- und Energieunternehmen bleiben, insbesondere, da die diplomatischen Bemühungen zur Wiederbelebung des iranischen Atomabkommens schwinden und Washington, Tel Aviv und Teheran nach alternativen Maßnahmen zur Erzwingung von Zugeständnissen suchen.

Angriffe Irans auf kritische Infrastruktur nach Land



Iranische Angriffe auf kritische Infrastruktur erfolgten vor allem gegen israelische, emiratische und US-amerikanische Organisationen.

Iranische Akteure werden im kommenden Jahr wahrscheinlich eine Bedrohung für die Verkehrs- und Energieunternehmen in den USA und Israel bleiben.

Iranische Gruppen haben ihre Ransomware-Angriffe über regionale Gegner hinaus ausgeweitet und nehmen prominente kritische Infrastruktur in den USA und in Israel ins Visier.

Umsetzbare Insights

1. Verbessern Sie die allgemeine Cyberhygiene Ihres Unternehmens, indem Sie kennwortlose Lösungen wie MFA aktivieren und deren Verwendung für alle Remote-Verbindungen erzwingen, um die Gefahr durch potenziell kompromittierte Anmeldeinformationen abzuschwächen.
2. Prüfen Sie die Authentizität des gesamten eingehenden E-Mail-Verkehrs, um sicherzustellen, dass die Absenderadresse legitim ist.
3. Patchen Sie frühzeitig und häufig.[34]
4. Überprüfen und überwachen Sie jede Ihrer Partnerbeziehungen mit Dienstanbietern, um unnötige Berechtigungen zwischen Ihrem Unternehmen und den vorgelagerten Anbietern zu minimieren. Microsoft empfiehlt, den Zugriff für alle Partnerbeziehungen, die unbekannt wirken oder noch nicht geprüft wurden, sofort zu entfernen.[35]

Links zu weiteren Informationen

- Iranian targeting of IT sector on the rise | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit (DSU)
- Iran-linked DEV-0343 targeting defense, GIS, and maritime sectors | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit (DSU)

Gruppe aus dem Libanon mit Verbindungen zum Iran nimmt Israel ins Visier

Microsoft überwacht Cyberbedrohungen unabhängig von der Plattform, dem angegriffenen Ziel oder der geografischen Region. Wir pflegen die Transparenz und halten das weltweite Threat-Hunting aufrecht, um für unsere Kunden bessere Erkennungsberichte zu schreiben.

Auch wenn Bedrohungen aus Russland, China, dem Iran und Nordkorea den Großteil der von uns beobachteten Aktivität von nationalstaatlichen Akteuren ausmachen, kommunizieren wir auch Bedrohungen aus NATO-Mitgliedstaaten und demokratischen Ländern. Im letzten Jahr haben wir über die Aktivität eines in der Türkei angesiedelten Akteurs (SILICON) sowie über die eines Akteurs aus Vietnam (BISMUTH) berichtet. In diesem Jahr betrachten wir die Details einer libanesischen Gruppe, die wir zuvor öffentlich enttarnt hatten.[36]

Microsoft deckte eine bisher undokumentierte, im Libanon ansässige Gruppe auf, bei der wir mit moderater Sicherheit davon ausgehen, dass sie mit Akteuren zusammenarbeitet, die ihrerseits mit dem Iranischen Ministerium für Aufklärung und Sicherheit (Ministry of Intelligence and Security, MOIS) in Verbindung stehen. Eine solche Zusammenarbeit oder Anweisungen aus Teheran würden zu Enthüllungen seit Ende 2020 passen, dass die iranische Regierung Dritte für die Ausführung ihrer Cyberoperationen einsetzt, vermutlich um dem Iran eine bessere Chance für eine plausible Abstreitbarkeit zu geben.

In der beobachteten Aktivität attackierte oder kompromittierte POLONIUM zwei Dutzend israelische Organisationen und eine IGO. Die entsprechenden Operationen erfolgten zwischen Februar und Mai 2022 im Libanon, bevor Microsoft diese Aktivität unterband und öffentlich enthüllte. Fast die Hälfte der israelischen Organisationen gehörten zur israelischen Rüstungsindustrie oder hatten Verbindungen zu israelischen Rüstungsunternehmen. Dies deutet darauf hin, dass die Interessen der Gruppe am Sammeln von Informationen und/oder an der Bekämpfung von Israel denen des Iran ähnelten.[37]

Die geprüften Links von POLONIUM zu MOIS-Gruppen basieren auf beobachteten Überschneidungen der Opfer sowie auf den Gemeinsamkeiten bei den verwendeten Tools und Techniken.

- Überschneidungen der Opfer: Eine staatliche iranische Gruppe mit Verbindungen zum iranischen MOIS wird von Microsoft als MERCURY verfolgt und hat zuvor mehrere Opfer von POLONIUM kompromittiert, was auf eine Übereinstimmung der Zielsetzungen beider Gruppen oder eine mögliche „Weitergabe" der Opfer zwischen ihnen hindeutet.
- Gemeinsame Tools und Techniken: Ähnlich wie bei POLONIUM hat MSTIC bei DEV-0588 (auch bekannt als CopyKittens) die häufige Verwendung von AirVPN bei ihren Operationen beobachtet, und bei DEV-0133 (auch bekannt als Lyceum[38]) wurde OneDrive für C2 und Exfiltrierung genutzt. Ähnlich wie die staatlichen iranischen Akteure nutzte POLONIUM einen Cloud-Dienstanbieter für die Kompromittierung eines israelischen Luftfahrtunternehmens und einer Anwaltskanzlei.[39]

Mithilfe von Cloud-Diensten für C2 und Datenfilterung hat POLONIUM eine Reihe von individuellen Implantaten bereitgestellt, insbesondere bei OneDrive und Dropbox. POLONIUM hat oft individuelle OneDrive-Anwendungen für Ziele entwickelt, die sich wahrscheinlich der Erkennung entziehen.

Mit Stand Juni 2022 hat Microsoft mehr als 20 der von POLONIUM erstellten OneDrive-Anwendungen vom Netz genommen, die betroffenen Organisationen benachrichtigt und eine Reihe von Security Intelligence-Updates bereitgestellt, um die von POLONIUM entwickelten Tools zu isolieren.

Microsoft hat den Missbrauch von OneDrive als C2 durch POLONIUM erfolgreich erkannt und unterbunden.

Umsetzbare Insights

1. Aktualisieren Sie Antivirustools,[40] und stellen Sie sicher, dass der Cloudschutz[41] aktiviert ist, um die entsprechenden Indikatoren zu erkennen.
2. Stellen Sie bei Kunden mit Beziehungen zu Dienstanbietern sicher, dass alle Partnerbeziehungen überprüft und überwacht werden, um unnötige Berechtigungen zwischen Ihrem Unternehmen und den vorgelagerten Anbietern zu minimieren.[42] Entfernen Sie sofort den Zugriff für alle Partnerbeziehungen, die unbekannt wirken oder noch nicht geprüft wurden.

Links zu weiteren Informationen

- Exposing POLONIUM activity and infrastructure targeting Israeli organizations | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit (DSU)
- MERCURY leveraging Log4j 2 vulnerabilities in unpatched systems to target Israeli organizations | Microsoft Threat Intelligence Center (MSTIC), Microsoft 365 Defender Research Team, Microsoft Defender Threat Intelligence

Nordkorea nutzt seine Cyberfähigkeiten, um die drei Hauptziele des Regimes zu erreichen

Im vergangenen Jahr spiegelten Nordkoreas Prioritäten im Cyberspace die von der Regierung verkündeten globalen Prioritäten wider. Kim Jong Un sprach die drei Prioritäten in mehreren wichtigen Reden an: Ausbau der Verteidigungskapazitäten, Stärkung der kriselnden Wirtschaft des Landes und Sicherstellung der inneren Stabilität.[43] Die von den staatlichen nordkoreanischen Akteuren getroffenen Maßnahmen zeigen deutlich, dass der Cyberspace zum Erreichen dieser drei Ziele genutzt wird.

Staatliche nordkoreanische Akteure nutzten eine Vielzahl von Taktiken, um zu versuchen, in Luft- und Raumfahrtunternehmen auf der ganzen Welt einzudringen.

Staatliche nordkoreanische Gruppen, vor allem CERIUM und ZINK, nutzten eine Vielzahl von Taktiken, um zu versuchen, Netzwerke von Rüstungs- und Luftfahrtunternehmen auf der ganzen Welt zu penetrieren. Als Nordkorea in der ersten Jahreshälfte 2022 die bisher aggressivste Phase seines Raketentests einleitete, nutzte es Cyberspionage, um den nordkoreanischen Forschenden einen Vorteil bei der Entwicklung eines eigenen Verteidigungssystems und von Gegenmaßnahmen gegen die Fortschritte seiner Kontrahenten zu verschaffen.

Wir haben beobachtet, wie COPERNICIUM eine Vielzahl von Unternehmen auf der ganzen Welt, die mit Kryptowährungen in Zusammenhang stehen, häufig mit Erfolg angriff, um der kriselnden Wirtschaft Nordkoreas zu helfen. Wir können zwar nicht bestätigen, ob die Gruppe nach einer Kompromittierung Gelder abziehen konnte, aber wir haben beobachtet, wie COPERNICIUM Dutzende von Computern infizierte, indem die Gruppe manipulierte Dokumente verschickte, die als Angebote von anderen Kryptowährungsunternehmen getarnt waren.

Und schließlich hat eine Gruppe, die Microsoft als DEV-0215 führt, daran gearbeitet die Stabilität und Regierungstreue in Nordkorea aufrechtzuerhalten. Dazu hat sie Nachrichtenunternehmen angegriffen, die über nordkoreanische Angelegenheiten berichten. Diese Nachrichtenmedien haben sowohl in Nordkorea als auch unter Überläufern Quellen, was Pjöngjang als existenzielle Bedrohung betrachtet. Darüber hinaus arbeitete die Gruppe daran, Zugang zu Netzwerken von koreanischsprachigen christlichen Gruppen zu erhalten, die in der Regel gegen Nordkorea eingestellt sind und aktiv mit nordkoreanischen Überläufern zusammenarbeiten.

Angriffe auf Rüstungs- und Luftfahrtunternehmen

Angeführt von CERIUM und ZINK betrieben staatliche nordkoreanische Akteure erheblichen Aufwand zur Entwicklung von Taktiken, die auf die Penetration von Rüstungs- und Luftfahrtunternehmen abzielen. CERIUM hat wiederholt südkoreanische VPNs (Virtual Private Networks) getestet, indem die Gruppe deren Clients heruntergeladen und auf Schwachstellen untersucht hat. Sie hat auch gängige Anwendungen heruntergeladen, die von Kund*innen des südkoreanischen Militärs und der Regierung verwendet werden, vermutlich ebenfalls, um nach Schwachstellen zu suchen. Die Gruppe verfolgte aktuelle Ereignisse genau und schrieb neue Köderdokumente, die vielbeachtete Themen nutzten, um die Ziele zum Klicken auf ihre ausführbaren Schadsoftware-Dateien bzw. bösartige Links zu verleiten.

Sowohl ZINK als auch CERIUM setzen bei ihren Kampagnen Social Media und Social Engineering ein. ZINK erwies sich als besonders geschickt beim Erstellen falscher Profile auf LinkedIn und anderen beruflichen Social-Netzwerken. Dabei gaben sich die Kriminellen als Personalverantwortliche von großen Rüstungs- und Luftfahrtunternehmen aus. Über diese Profile versendeten sie Links oder bösartige Dateianhänge an potenzielle Opfer. Dazu verwendeten sie die Messenger in den sozialen Netzwerken oder E-Mails.

Neben Mitarbeiter*innen von Unternehmen nahm CERIUM auch breiter gefasste Angehörige des südkoreanischen Militärs ins Visier. Ein besonderes Interesse zeigen sie sowohl an südkoreanischen Militärakademien als auch an Militärangehörigen, die im akademischen Bereich tätig waren.

Angriffe auf Kryptowährungen zum Ausgleich von Verlusten

Seit dem Verhängen der Sanktionen im Jahr 2016 ist die nordkoreanische Wirtschaft weiter geschrumpft, verschärft durch Naturkatastrophen wie Überschwemmungen[44] und Dürre[45] sowie durch eine fast vollständige Schließung der Grenzen für Importe seit dem Ausbruch der COVID-19-Pandemie Anfang 2020.[46] Zwar hatte Nordkorea seine Grenzen Anfang 2022 für den Handel mit China kurzzeitig geöffnet, aber bald wieder geschlossen.[47] Mitte Mai meldete Nordkorea seinen ersten inländischen Fall von COVID-19.[48] Seitdem hat es eine Zero-COVID-Strategie im Stile Chinas verfolgt, die das Virus mit Massen-Lockdowns zu bekämpfen versucht, was negative Folgen für die ohnehin schon fragile Wirtschaft Nordkoreas hatte.

Die staatliche nordkoreanische Gruppe COPERNICIUM hat versucht, einen Teil der verlorenen Einnahmen durch den Diebstahl von Geldern – üblicherweise in Form von Kryptowährungen – von jedem Unternehmen, dessen Netzwerk sie penetrieren konnte, auszugleichen. Wir haben Dutzende kompromittierte Computer verzeichnet, die zu mit Kryptowährungen befassten Unternehmen in den USA, in Kanada, in Europa und in ganz Asien gehörten. COPERNICIUM griff sogar Computer von Kryptowährungsunternehmen in Nordkoreas stärkstem Verbündeten China an, sowohl auf dem Festland als auch in Hongkong. Die Gruppe stützte sich bei ihrer Frühaufklärung und bei der Kontaktaufnahme mit Zielen stark auf soziale Netzwerke. Die Akteure erstellten Profile, die vorgaben, zu Entwickler*innen oder Führungskräften in mit Kryptowährung befassten Branchen zu gehören. Dann versuchten sie, Beziehungen mit Personen in diesen Branchen aufzubauen und, sobald ausreichend Vertrauen hergestellt war, bösartige Links oder Dateien an sie zu senden.

Nordkorea nutzt seine Cyberfähigkeiten, um die drei Hauptziele des Regimes zu erreichen

Fortsetzung

Eine Gruppe mit Verbindungen zu PLUTONIUM entwickelt Ransomware und stellt sie bereit

Eine Gruppe von Akteuren aus Nordkorea, die Microsoft als DEV-0530 verfolgt, begann im Juni 2021 damit, Ransomware zu entwickeln und bei ihren Angriffen einzusetzen. Diese Gruppe, die sich selbst H0lyGh0st nannte, nutzte für ihre Kampagnen eine Ransomware-Nutzlast gleichen Namens und kompromittierte bereits im September 2021 kleine Unternehmen in mehreren Ländern.

Microsoft geht davon aus, dass DEV-0530 Verbindungen zu einer weiteren nordkoreanischen Gruppe hatte, die als PLUTONIUM (auch bekannt als DarkSeoul oder Andariel) geführt wird. Während die Verwendung von H0lyGh0st-Ransomware in Kampagnen ein Alleinstellungsmerkmal von DEV-0530 ist, beobachtete MSTIC eine Kommunikation zwischen den beiden Gruppen und verfolgte außerdem, wie DEV-0530 Tools verwendete, die ausschließlich von PLUTONIUM erstellt wurden.

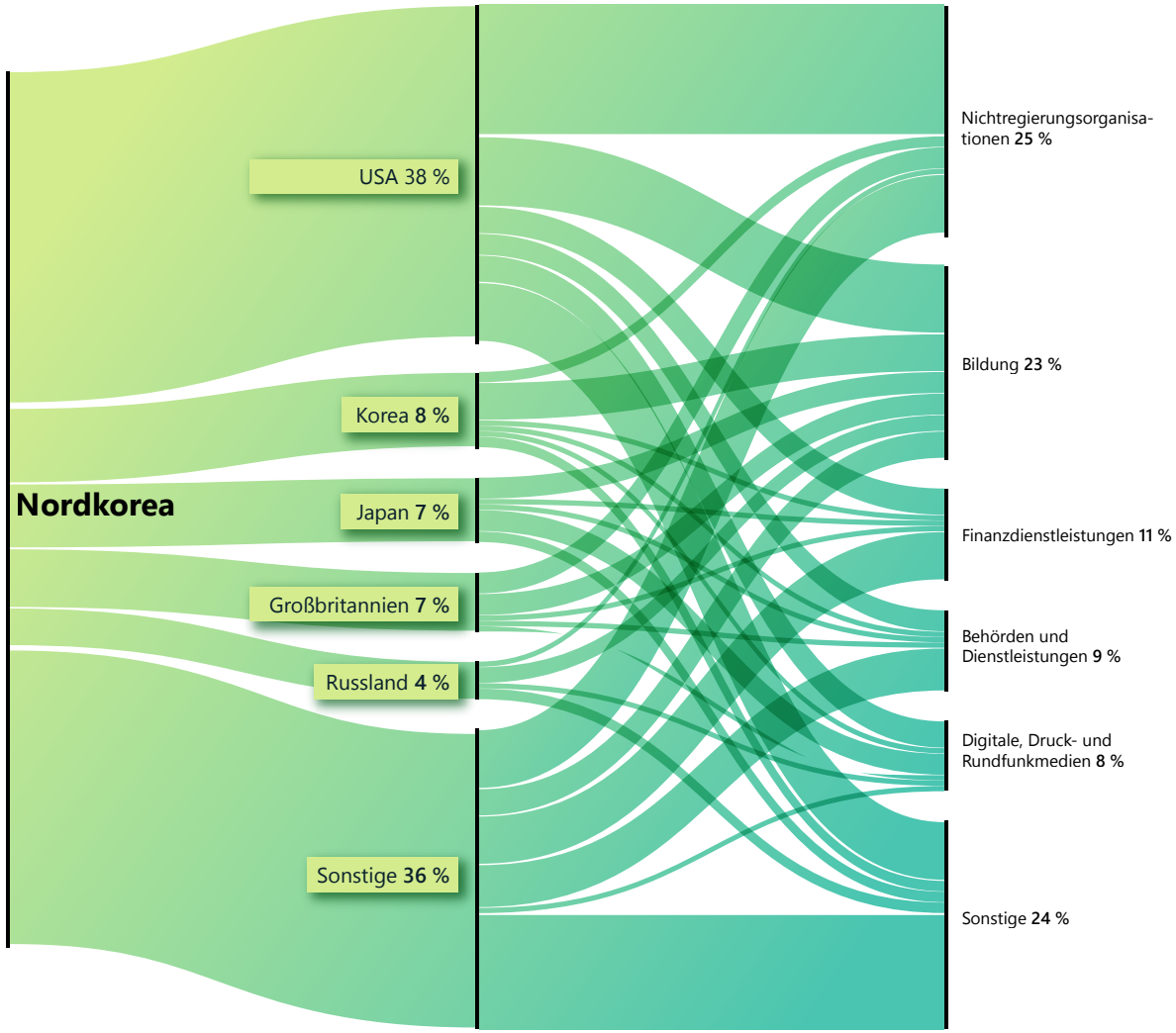
Es ist nicht sicher, dass die Aktivitäten von DEV-0530 staatlich gesponsert wurden. Auch wenn die Ransomware-Angriffe von der Regierung aus dem gleichen Grund in Auftrag gegeben worden sein konnten, aus dem sie auch hinter dem Bestehlen von Kyptowährungsunternehmen steckt, kann es auch sein, dass die Akteure hinter DEV-0530 eigenständig gehandelt haben, um Geld für sich selbst zu erpressen. Sollten es unabhängige nordkoreanische Hacker gewesen sein, würde dies erklären, warum die Aktivität im Gegensatz zu den staatlich beauftragten Raubzügen bei den Kryptowährungsunternehmen nicht breit angelegt war.

Angriffe auf nordkoreanische Nachrichtenmedien, Überläufer, religiöse Gruppen und Hilfsorganisationen

Im letzten Jahr konzentrierte sich Kim Jong Un in der Öffentlichkeit mehr auf innere Sicherheit und Staatstreue als auf Raketen und Nuklearwaffen. Im Lichte dieser innenpolitischen Probleme konzentrierten sich mindestens zwei staatliche nordkoreanische Gruppen auf Aspekte, die das Regime als innenpolitische Bedrohungen ansehen würde.

Die erste Gruppe verfolgt Microsoft als DEV-0215. Sie greift Medienorganisationen an, die die nordkoreanische Nachrichtenlage genau verfolgen. Ein wahrscheinlicher Grund für diese Angriffe besteht darin, dass die Nachrichtenmedien ihre Meldungen von nordkoreanischen Überläufern erhalten sowie von chinesischen Bürgern, die eng mit Nordkorea zusammenarbeiten, oder sogar von nordkoreanischen Bürgern innerhalb des Landes, die vielfältige Methoden für die Kommunikation mit der Außenwelt nutzen. Die nordkoreanische Regierung betrachtet diese Gruppen als existenzielle Bedrohung für ihr Überleben. Das gilt insbesondere für Bürger innerhalb Nordkoreas, die als Verräter und Spione betrachtet werden würden. DEV-0215 versuchte vermutlich, die Quellen dieser Nachrichtenorganisationen ausfindig zu machen, um potenzielle Informationslecks zu neutralisieren.

Nordkorea: die fünf am häufigsten angegriffenen Länder und Industriezweige



Nordkorea betrachtet die Vereinigten Staaten, Südkorea und Japan als seine vorrangigen Feinde. Obwohl Russland ein langjähriger Verbündeter ist, greifen nordkoreanische Akteure auch russische Thinktanks, Akademiker*innen und diplomatische Vertreter*innen an, um Informationen über die russischen Meinungen zu globalen Angelegenheiten zu erhalten.

Nordkorea nutzt seine Cyberfähigkeiten, um die drei Hauptziele des Regimes zu erreichen

Fortsetzung

Microsoft fand auch Beweise dafür, dass DEV-0215 koreanischsprachige christliche Gemeinden angegriffen hat. Evangelische Christlich-Koreanische Kirchen haben für gewöhnlich eine kritische Haltung sowohl gegenüber Nordkorea als auch südkoreanischen Regierungen, die einen Austausch mit Nordkorea befürworten. Es ist wahrscheinlich, dass diese Kirchen Kontakt zu Überläufern aufnehmen, und einige haben bei humanitärer Arbeit mit Nordkorea zu tun. Nordkorea betrachtet sie als Bedrohung. Denn, obwohl der Strom von Überläufer*innen aus Nordkorea während der Pandemie fast vollständig ausgetrocknet ist,[49] spielen diese christlichen Gruppen häufig eine wichtige Rolle bei der Fluchthilfe für Überläufer*innen. DEV-0215 hat gefälschte Dokumente über christliche Konferenzen als Köder für koreanische Referent*innen erstellt, um die Gruppe anzugreifen und herauszufinden, wer bei der Organisation von Fluchten von Überläufer*innen hilft.

Und schließlich zeigte die staatliche Gruppe OSMIUM über das ganze Jahr hinweg ein konstantes Interesse an internationalen Hilfsorganisationen, einschließlich Organisationen, die Nordkorea in der Vergangenheit geholfen haben. Auch wenn Nordkorea Hilfsangebote von außerhalb des Landes in der gemieden hat, insbesondere seit dem Ausbruch von COVID-19,[50] kann es trotzdem sein, dass das Land die Annahme von Hilfe in Erwägung zieht. Allerdings ist es besorgt über die Folgen für die Sicherheit, die das Zulassen ausländischer Hilfskräfte im Land nach sich ziehen könnte. Nordkorea könnte in die Netzwerke von Hilfsorganisationen auf der ganzen Welt eindringen, um zu ermitteln, ob es solche Hilfe im eigenen Land zulassen sollte.

Umsetzbare Insights

1. Staatliche nordkoreanische Akteure sind kompetent, hartnäckig und kreativ, doch Organisationen können sich gegen sie wehren.

2. Die erfolgreichsten Angriffe lassen sich mit grundlegender Cyberhygiene stoppen, z. B. durch Multi-Faktor-Authentifizierung oder die Vermeidung des Öffnens von Dateianhängen, die von unbekannten Personen in einer virtuellen Umgebung stammen.

Links zu weiteren Informationen

- North Korean threat actor targets small and midsize businesses with H0lyGh0st ransomware | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit (DSU)

Unter den Expert*innen für Nordkorea herrscht seit langem eine Debatte darüber, ob die nordkoreanische Regierung es bei ihren öffentlichen Verlautbarungen aufrichtig meint oder nur auf Wirkung aus ist. Die Übereinstimmung der Cyberangriffe mit den von Nordkorea verkündeten Prioritäten stützt die Meinung, dass Nordkorea meint, was es sagt, wenn es öffentlich über seine Ziele spricht.

Cybersöldner bedrohen die Stabilität des Cyberspace

Es gibt eine wachsende Wirtschaft mit privaten Unternehmen, die Tools, Techniken und Services entwickeln und verkaufen, mit denen ihre Kunden – oft Regierungen – in Netzwerke, Computer, Telefon und Internetgeräte einbrechen können. Als Ressource für nationalstaatliche Akteure gefährden diese Entitäten häufig Dissidenten, Menschenrechtsaktivisten, Journalisten, Vertreter der Zivilgesellschaft und andere Privatpersonen. Wir nennen sie Cybersöldner oder offensive Akteure im privaten Sektor.

Eine Welt, in der privatwirtschaftliche Unternehmen Cyberwaffen entwickeln und verkaufen, ist noch gefährlicher für Verbraucher, Unternehmen aller Größen und Regierungen. Diese offensiven Tools können auf eine Weise verwendet werden, die mit den Normen und Werten einer guten Governance und Demokratie unvereinbar ist. Microsoft ist der Auffassung, dass der Schutz der Menschenrechte eine grundsätzliche Verpflichtung ist. Eine, die wir ernst nehmen, indem wir „Surveillance-as-a-Service“ auf der ganzen Welt bekämpfen.

Microsoft hat festgestellt, dass bestimmte staatliche Akteure, über demokratische und autoritäre Regime hinweg, die Entwicklung oder Verwendung von „Surveillance-as-a-Service“-Technologie auslagern. Auf diese Weise umgehen sie Verantwortlichkeit und Aufsicht und erwerben außerdem Funktionen, die sich eigenständig nur schwer entwickeln ließen.

> Diese Cyberwaffen versorgen Nationalstaaten mit Überwachungsfunktionen, die sie auf sich allein gestellt nicht hätten entwickeln können.

Der Markt, in dem Cybersöldner operieren, ist undurchsichtig. Dennoch beobachten wir weiterhin, wie diese Gruppen Zero-Day-Exploits und sogar Zero-Click-Exploits, die überhaupt keine Interaktion mit dem Opfer erfordern, verwenden und auf diese Weise Überwachung als Dienstleistung, also Surveillance-as-a-Service, ermöglichen.

Microsoft hat vor Kurzem einen europäischen offensiven Akteur im privaten Sektor enttarnt, den wir als KNOTWEED bezeichnen. Dabei handelt es sich um eine in Österreich ansässige Privatorganisation namens DSIRF. Mehrere Nachrichtenberichte bringen das Unternehmen mit der Entwicklung und dem versuchten Verkauf eines Schadsoftware-Toolsets namens Subzero in Verbindung.[51] Opfer sind Anwaltskanzleien, Banken und strategische Beratungsunternehmen in Ländern wie Österreich, Großbritannien und Panama.[52]

Weil solche offensiven Überwachungsfunktionen mittlerweile keine streng geheimen Funktionen mehr sind, die von Rüstungs- und Geheimdienstorganisationen entwickelt wurden, sondern kommerzielle Produkte, die Unternehmen und Einzelpersonen angeboten werden, muss jegliches Regulationssystem für Cyberwaffen über Exportkontrolle hinausgehen. Die Auswirkungen dieser Cyberwaffen können verheerend sein.

Wenn ein Cybersöldner eine Schwachstelle in einem Produkt oder Dienst ausnutzt, bringt er die gesamte Computing-Infrastruktur in Gefahr. Sobald Schwachstellen öffentlich bekannt werden, befinden sich die Unternehmen in einem Wettlauf gegen die Zeit, um Schutzmaßnahmen zu veröffentlichen, bevor breit angelegte Angriffe losgehen (siehe unsere Erörterung der Ausnutzung von Schwachstellen weiter oben). Dies ist ein gefährlicher und schwieriger Kreislauf sowohl für Softwareanbieter (die sinnvollerweise Patches entwickeln müssen) als auch für die Kunden von Produkten (die die Patches sofort implementieren müssen).

Als Gründungsmitglied von Cybersecurity Tech Accord[53] – einer führenden Allianz, die mehr als 150 Technologieunternehmen zusammenbringt – hat Microsoft sich verpflichtet, sich nicht an offensiven Onlineaktivitäten zu beteiligen. Wir stehen zu dieser Verpflichtung und zu unser diesbezüglichen Verantwortung für die Menschenrechte. Wir haben uns mit technischen Gegenmaßnahmen und rechtlichen Herausforderungen befasst, um die negativen Auswirkungen der von Cybersöldnern angebotenen Dienstleistungen zu beleuchten, und werden weiterhin unsere Kund*innen schützen, wenn wir einen Missbrauch bemerken.

> Cybersöldner*innen erstellen und bieten „Surveillance-as-a-Service"-Funktionen, die technologisch ausgereift und allgemein verfügbar sind. Dies umfasst auch fortschrittliche Schadsoftware und eine Reihe von Techniken.

Umsetzbare Insights für staatliche Einrichtungen

1. Implementieren Sie Transparenz- und Aufsichtsanforderungen für Surveillance-as-a-Service, insbesondere bei der Beschaffung. Dazu sollte auch die Aussperrung dieser feindseligen Akteure gehören, wie es die USA mit den Unternehmen auf der Handelsbeschränkungsliste („Entity List“) des US-Wirtschaftsministeriums getan haben.
2. Etablieren Sie für Mitarbeiter*innen in diesem Sektor Einschränkungen nach dem Ausscheiden aus der Organisation.
3. Verfolgen Sie das Ziel von „Know your Customer“, und halten Sie Unternehmen an, sich an ihre Verpflichtungen in Bezug auf die Menschenrechte zu halten.

Links zu weiteren Informationen

- Untangling KNOTWEED: European private-sector offensive actor using 0-day exploits | Microsoft Threat Intelligence Center (MSTIC), Microsoft Security Response Center (MSRC), RiskIQ (Microsoft Defender Threat Intelligence)
- Continuing the fight against private sector cyberweapons | Microsoft On the Issues

Umsetzung von Standards zur Cybersicherheit für Frieden und Sicherheit im Cyberspace

Wir brauchen dringend einen einheitlichen, globalen Rahmen, der die Menschenrechte priorisiert und Menschen vor rücksichtslosem staatlichen Verhalten im Cyberraum schützt. Nirgendwo wird uns dies deutlicher vor Augen geführt, als im laufenden Krieg in der Ukraine. Neben einer globalen strategischen Anstrengung können Regierungen jetzt handeln, um einen direkten positiven Effekt zu bewirken.

Vor fünf Jahren forderte Microsoft eine „digitale Genfer Konvention", um die Verantwortung und die Pflichten in allen Bereichen zu verbessern und dadurch Frieden und Sicherheit online zu verteidigen. Der Cyberspace ist zu einem eigenen und volatilen Gebiet von Konflikt und Konkurrenz zwischen Staaten geworden, und die Angreife werden zahlreicher – selbst in Friedenszeiten.

Auch heute gibt es noch einen eindeutigen Bedarf für so einen Rahmen – belegt durch die russischen Cyberangriffe gegen die Ukraine als Teil des russischen Angriffskriegs. Dieser Krieg hat eine neue Front geschaffen, die sich drastisch von allen bisher bekannten unterscheidet.

Um den Cyberspace zu stabilisieren, bedarf es einer Stärkung und eines Neudenkens der Institutionen für Global Governance, damit sie ihre Aufgaben erfüllen können. Der Cyberspace unterscheidet sich grundlegend von anderen Domänen – er ist grenzenlos, künstlich und wird größtenteils von der Privatwirtschaft unterhalten. Dies bedeutet, dass die Technologiebranche mehr Verantwortung für die Sicherheit von Produkten und Diensten sowie für die breiter gefasste digitale Infrastruktur übernehmen muss. Auch wenn an allen Fronten bemerkenswerte Fortschritte erzielt wurden, haben die Herausforderungen dramatisch zugenommen.

Um die Sicherheit des Cyberspace zu verteidigen, müssen wir die gemeinsamen Anstrengungen verdoppeln. Wir können die Rechte und Freiheiten, an die wir uns online gewöhnt haben, nicht für selbstverständlich halten. Während wir noch mit den gegebenen Herausforderungen beschäftigt sind, planen böswillige Akteure bereits, wie und wo sie als Nächstes zuschlagen werden. Dafür setzen sie KI zur Desinformation ein und suchen nach Wegen, um das neue Metaverse zu untergraben. Menschenrechtsaktivisten, die Technologiebranche und Regierungen, die die Rechte respektieren, müssen gemeinsam auf eine positive Vision einer sicheren und geschützten Onlinewelt hinarbeiten. Der Weg in die Zukunft ist lang, doch es gibt Dinge, die Regierungen jetzt tun können, die Sicherheitsinfrastruktur des Cyberspace unmittelbar zu verbessern.

- In Zuschreibungen müssen Normen, Gesetze und Konsequenzen genannt werden. Eine wesentliche Verbesserung der letzten fünf Jahre bestand in der Geschwindigkeit und der Koordination der staatlichen Zuschreibungen von Cyberangriffen. Neben der bloßen Namensnennung und der Enttarnung müssen diese Aussagen hervorheben, welche internationalen Gesetze oder Normen verletzt wurden und welche Konsequenzen verhängt werden, um die Anerkennung der internationalen Erwartungen zu stärken.
- Es muss geklärt werden, wie das internationale Recht online auszulegen ist. Die Regierungen sind sich zwar darüber einig, dass das internationale Recht auch online gilt, doch es bleiben Fragen in Bezug darauf, wie es online in bestimmten Fällen anzuwenden ist. Dies ist insbesondere im Nachgang des Angriffskriegs gegen die Ukraine relevant. Regierungen stehen viele Möglichkeiten offen, Erwartungen zu formen, Missverständnisse zu vermeiden und Vertrauen aufzubauen, indem sie deutlich machen, wie sie ihre Verpflichtungen unter internationalem Recht verstehen.
- Es muss enge Beratungen mit anderen Stakeholdern geben. Internationale Foren bieten weiterhin die beste Möglichkeit, um auszuloten, wie sich eine solide Einbindung mehrerer Stakeholder bewerkstelligen lässt. Regierungen können einen fachkundigen Austausch innerhalb von Communitys mit mehreren Stakeholdern, insbesondere aus der Technologiebranche, fördern, um dafür zu sorgen, dass der Austausch vom unschätzbaren Fachwissen einiger Teilnehmer profitiert.
- Es sollte ein ständiges Gremium für verantwortungsbewusstes staatliches Verhalten im Cyberspace geformt werden. Die Arbeit internationaler diplomatischer Foren an einer Förderung von verantwortungsvollem staatlichen Verhalten war niemals wichtiger. Es besteht ein eindeutiger Bedarf an einem permanenten UN-Mechanismus, um mit dem Cyberspace als Konfliktgebiet umzugehen.
- Für sich entwickelnde Bedrohungen müssen neue Normen definiert werden. Bedrohungen im Cyberspace entwickeln sich gleichzeitig mit technologischen Innovationen beständig weiter. Auch wenn internationale Normen technologieneutral sein sollten, müssen sie aktualisiert und an die Veränderungen in der Bedrohungslandschaft und unseren Umgang mit Technologie angepasst werden. Selbst heute erleben wir, wie Lücken im vorhandenen internationalen Rahmenwerk ausgenutzt werden. Staaten sollten sich dazu verpflichten, Kernprozesse, die Grundpfeiler der zurzeit ungeschützten digitalen Infrastruktur sind, z. B. der Softwareupdateprozess, ausdrücklich zu schützen. Darüber hinaus verdienen bestimmte Bereiche zusätzlichen Schutz. Mitten in der Pandemie haben wir beispielsweise gelernt, dass Normen für den Schutz der Gesundheitsversorgung unerlässlich sind.

Nationalstaatliche Akteure und Angriffe nehmen an Volumen und Raffinesse zu und schaffen so eine unhaltbare Situation.

Sofortiges Handeln ist unerlässlich – es gibt Dinge, die Regierungen sofort unternehmen können, um die Infrastruktur für Cybersicherheit zu verbessern. Dazu gehört das Implementieren vereinbarter Normen und Regeln für staatliches Verhalten im Cyberspace sowie die Zusammenarbeit mit der breiten Community aus mehreren Stakeholdern beim Schließen von entstehenden Sicherheitslücken.

Multilaterale Institutionen müssen neu gedacht werden, um die drängenden Herausforderungen nationalstaatlicher Cyberattacken zu bewältigen.

Links zu weiteren Informationen

- A moment of reckoning: the need for a strong and global cybersecurity response | Microsoft On the Issues
- Cyberattacks targeting health care must stop | Microsoft On the Issues
- The next chapter of cyber diplomacy at the United Nations beckons | Microsoft On the Issues

Fußnoten

1. https://www.microsoft.com/en-us/cybersecurity/content-hub/cloud-security
2. https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks/
3. Kritische Infrastruktur wird in diesem Kapitel definiert durch die Presidential Policy Directive 21 (PPD-21), Critical Infrastructure Security and Resilience (Februar 2013).
4. https://www.microsoft.com/security/blog/2021/11/18/iranian-targeting-of-it-sector-on-the-rise/
5. https://www.microsoft.com/security/blog/2022/06/02/exposing-polonium-activity-and-infrastructure-targeting-israeli-organizations/
6. https://www.microsoft.com/security/blog/2021/10/25/nobelium-targeting-delegated-administrative-privileges-to-facilitate-broader-attacks/
7. https://www.microsoft.com/en-us/security/business/identity-access/azure-active-directory-passwordless-authentication
8. https://www.solarwinds.com/trust-center/security-advisories/cve-2021-35211
9. https://pitstop.manageengine.com/portal/en/community/topic/adselfservice-plus-6114-security-fix-release
10. https://reliefweb.int/report/ukraine/unicef-ukraine-humanitarian-situation-report-no-13-10-17-may-2022
11. https://news.un.org/en/story/2022/06/1119672
12. https://zetter.substack.com/p/dozens-of-computers-in-ukraine-wiped?s=r ; https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/
13. https://www.cnn.com/2022/03/14/economy/china-jan-feb-economy-challenges-ahead-intl-hnk/index.html
14. https://www.wsj.com/articles/russias-vladimir-putin-meets-with-chinese-leader-xi-jinping-in-beijing-11643966743
15. https://www.washingtonpost.com/world/2022/04/01/china-eu-summit/
16. https://twitter.com/MoNDefense
17. https://news.usni.org/2022/01/24/2-u-s-aircraft-carriers-now-in-south-china-sea-as-chinese-air-force-flies-39-aircraft-near-taiwan
18. https://ec.europa.eu/trade/policy/in-focus/eu-china-agreement/; https://www.usnews.com/news/world/articles/2022-02-28/eu-plans-summit-with-china-on-april-1-to-address-tensions
19. https://www.wsj.com/articles/u-s-on-sidelines-as-china-and-other-asia-pacific-nations-launch-trade-pact-11641038401
20. https://greenfdc.org/chinas-two-sessions-2022-what-it-means-for-economy-climate-biodiversity-green-finance-and-the-belt-and-road-initiative-bri/
21. https://www.cfr.org/global-conflict-tracker/conflict/territorial-disputes-south-china-sea
22. https://www.theguardian.com/world/2022/apr/30/the-china-solomons-security-deal-has-been-signed-time-to-move-on-from-megaphone-diplomacy
23. https://www.fmprc.gov.cn/eng/zxxx_662805/202205/t20220531_10694928.html
24. https://blogs.microsoft.com/on-the-issues/2021/12/06/cyberattacks-nickel-dcu-china/; https://www.microsoft.com/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe/
25. https://www.microsoft.com/security/blog/2022/04/12/tarrask-malware-uses-scheduled-tasks-for-defense-evasion/
26. https://attack.mitre.org/techniques/T1053/
27. https://www.microsoft.com/security/blog/2022/07/26/malicious-iis-extensions-quietly-open-persistent-backdoors-into-servers/
28. https://www.microsoft.com/security/blog/2021/02/11/web-shell-attacks-continue-to-rise/
29. https://www.timesofisrael.com/in-rare-criticism-of-irgc-rouhani-slams-anti-israel-slogans-on-test-missiles/; https://www.theguardian.com/world/2017/may/05/iran-president-hassan-rouhani-nuclear-agreement-sabotaged; https://d2071andvip0wj.cloudfront.net/184-iran-s-priorities-in-a-turbulent-middle-east_1.pdf; https://www.aljazeera.com/news/2016/3/9/iran-launches-ballistic-missiles-during-military-drill; https://www.usatoday.com/story/news/world/2015/04/25/iran-yemen-weapons/26367493/; https://www.armscontrol.org/blog/ArmsControlNow/2016-03-14/The-Iranian-Ballistic-Missile-Launches-That-Didnt-Happen; https://www.reuters.com/world/middle-east/iran-parliament-approves-most-raisi-nominees-hardline-cabinet-2021-08-25/;
30. https://www.reuters.com/world/middle-east/iran-parliament-approves-most-raisi-nominees-hardline-cabinet-2021-08-25/; https://www.france24.com/en/live-news/20210825-iran-s-parliament-approves-president-s-cabinet-choices

Fußnoten, Fortsetzung

31. https://www.janes.com/defence-news/news-detail/iranian-irgc-consolidates-primacy-inintelligence-operations; https://www.proofpoint.com/us/blog/threat-insight/badblood-ta453-targets-us-and-israeli-medical-research-personnel-credential; https://miburo.substack.com/p/iran-disinfo-privatized?s=r.
32. https://www.reuters.com/business/energy/iran-says-israel-us-likely-behind-cyberattack-gas-stations-2021-10-30/
33. https://www.tasnimnews.com/en/news/2021/11/05/2602361/us-military-action-off-the-table-iranian-general
34. Patchen Sie insbesondere ProxyShell-Schwachstellen auf Exchange Servern (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 und CVE-2021-27065, CVE-2021-34473). Achten Sie auch darauf, Fortinet-FortiOS SSL VPN-Geräte in Bezug auf Sicherheitslücken zu patchen.
35. https://docs.microsoft.com/en-us/microsoft-365/commerce/manage-partners?view=o365-worldwide
36. https://www.microsoft.com/security/blog/2022/06/02/exposing-polonium-activity-and-infrastructure-targeting-israeli-organizations/
37. https://www.microsoft.com/security/blog/2022/06/02/exposing-polonium-activity-and-infrastructure-targeting-israeli-organizations/
38. https://www.secureworks.com/blog/lyceum-takes-center-stage-in-middle-east-campaign
39. https://www.microsoft.com/security/blog/2021/11/18/iranian-targeting-of-it-sector-on-the-rise/
40. https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/manage-updates-baselines-microsoft-defender-antivirus?view=o365-worldwide
41. https://docs.microsoft.com/microsoft-365/security/defender-endpoint/cloud-protection-microsoft-defender-antivirus
42. https://docs.microsoft.com/microsoft-365/commerce/manage-partners?view=o365-worldwide
43. https://www.marketwatch.com/story/kim-jong-un-calls-for-improved-living-conditions-in-north-korea-01633920099
https://www.bbc.com/news/world-asia-59845636
https://kcnawatch.org/newstream/1650963237-449932111/respected-comrade-kim-jong-un-makes-speech-at-military-parade-held-in-celebration-of-90th-founding-anniversary-of-kpra/
44. https://www.theguardian.com/world/2021/aug/06/north-korea-homes-wreckeddamaged-and-and-bridges-washed-away-in-floods
45. https://www.reuters.com/world/asia-pacific/nkorea-mobilises-office-workers-fight-drought-amid-food-shortages-2022-05-04/
46. https://www.washingtonpost.com/world/asia_pacific/north-korea-kim-pandemic/2021/09/08/31adfd74-ff53-11eb-87e0-7e07bd9ce270_story.html
47. https://news.yahoo.com/china-halts-freight-train-traffic-102451425.html
48. https://www.cnn.com/2022/05/11/asia/north-korea-covid-omicron-coronavirus-intl-hnk/index.html
49. https://www.csis.org/analysis/number-north-korean-defectors-drops-lowest-level-two-decades
50. https://www.aljazeera.com/economy/2022/5/20/north-korea-shuns-outside-help-as-covid-catastrophe-looms
51. Jan-Philipp Hein, Im Rätsel um gruselige Spionage-Software führt die Spur über Wirecard in den Kreml, FOCUS Online (2022) https://www.focus.de/politik/vorab-aus-dem-focus-volle-kontrolle-ueber-zielcomputer-das-raetsel-um-die-spionage-app-fuehrt-ueber-wirecard-zu-putin_id_24442733.html; Sugar Mizzy, We unveil the "Subzero" state trojan from Austria, Europe-cities (2021) https://europe-cities.com/2021/12/17/we-unveil-the-subzero-state-trojan-from-austria/; Andre Meister, Wir enthüllen den Staatstrojaner „Subzero" aus Österreich, Netzpolitik.org (2022) https://netzpolitik.org/2021/dsirf-wir-enthuellen-den-staatstrojaner-subzero-aus-oesterreich.
52. Wie in unserem technischen Blog erwähnt, bedeutet die Identifizierung von Zielen in einem Land nicht unbedingt, dass sich die entsprechenden DSIRF-Kund*innen im selben Land befinden, weil internationale Angriffe üblich sind.
53. Startseite | Cybersecurity Tech Accord (cybertechaccord.org)

Geräte und Infrastruktur

Angesichts der Beschleunigung der digitalen Transformation ist die Sicherheit der digitalen Infrastruktur wichtiger denn je.

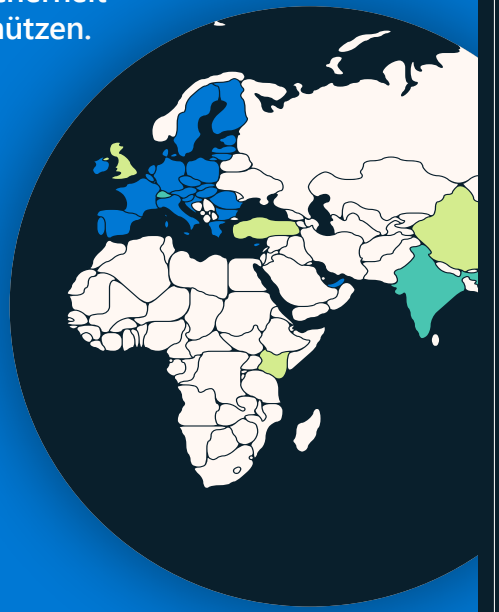
Übersicht über

Geräte und Infrastruktur

In Kombination mit der schnellen Einführung von Internetgeräten aller Art als eine Komponente zur Beschleunigung der digitalen Transformation hat die Pandemie die Angriffsfläche unserer digitalen Welt stark erhöht.

Cyberkriminelle und Nationalstaaten nutzen das schnell aus. Obwohl die Sicherheit von IT-Hardware und -Software in den letzten Jahren robuster geworden ist, konnte die Sicherheit von IoT (Internet of Things)- und OT (Operational Technology)-Geräten nicht damit Schritt halten. Akteure etablieren über solche Geräte Zugriff auf Netzwerke und ermöglichen laterale Bewegung, wodurch sie in einer Lieferkette Fuß fassen oder die OT-Abläufe der Zielorganisation stören können.

Weltweit bewegen sich Regierungen, um kritische Infrastruktur durch die Verbesserung von IoT- und OT-Sicherheit zu schützen.

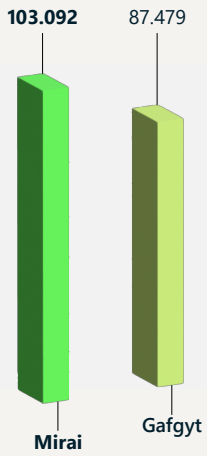


Weitere Informationen finden Sie auf S. 59

Global einheitliche und kompatible Sicherheitsrichtlinien sind nötig, um einen breiten Einsatz zu gewährleisten.

Weitere Informationen finden Sie auf S. 59

Malware-as-a-Service hat sich zu groß angelegten Operationen gegen exponiertes IoT und OT in Infrastruktur- und Energiebetrieben sowie gegen Unternehmensnetzwerke allgemein entwickelt.



Weitere Informationen finden Sie auf S. 63

Mit mehr als 100 Millionen beobachteten Angriffen im Mai 2022 nehmen Angriffe gegen Remote-Verwaltungsgeräte weiter zu. Damit hat sich der Anstieg im vergangenen Jahr verfünffacht.

Weitere Informationen finden Sie auf S. 62

Angreifer nutzen zunehmend Schwachstellen in der Firmware von IoT-Geräten, um Unternehmensnetzwerke zu infiltrieren und verheerende Angriffe zu starten.

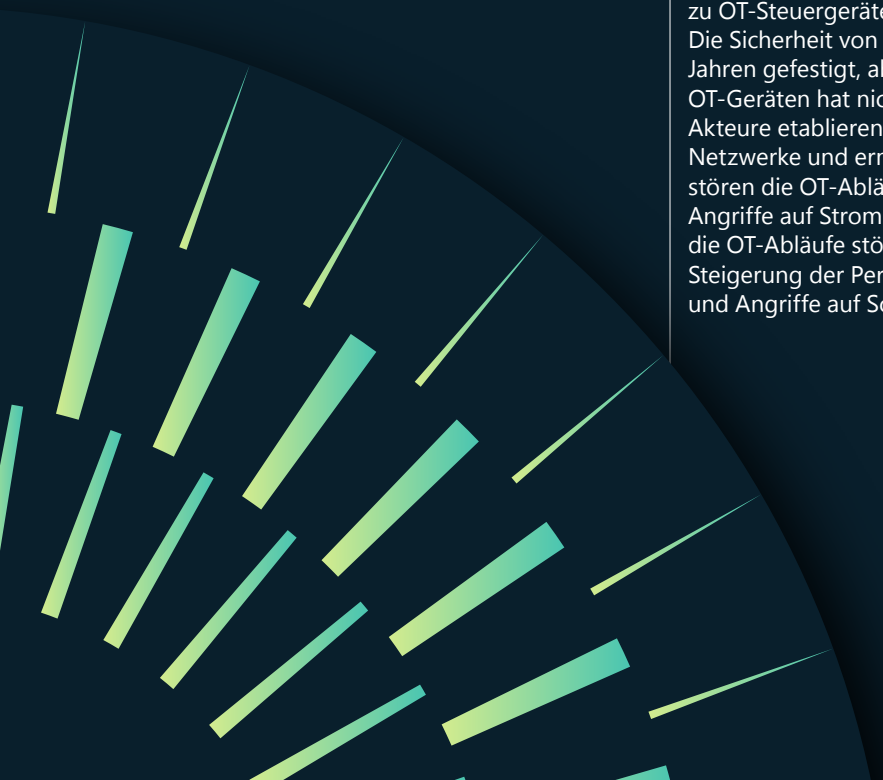
Weitere Informationen finden Sie auf S. 65

32 % der analysierten Firmware-Images enthielten mindestens 10 bekannte kritische Schwachstellen.

Weitere Informationen finden Sie auf S. 66

Einführung

Die Beschleunigung der digitalen Transformation hat das Cybersicherheitsrisiko für kritische Infrastruktur und andere physische Internetsysteme erhöht.



In den letzten Jahren hat sich die digitale Welt auf beispiellose Weise gewandelt. Unternehmen entwickeln sich weiter, um Fortschritte bei der Rechenleistung sowohl aus der intelligenten Cloud als auch aus dem Intelligent Edge auszuschöpfen. Die Pandemie hat Unternehmen und Organisationen praktisch zur Digitalisierung gezwungen, um ihren Erfolg zu sichern, und angesichts des Tempos, mit dem Branchen online verbundene Geräte einführen, nimmt die Angriffsfläche der digitalen Welt exponentiell zu.

Mit dieser schnellen Migration konnte die Sicherheitscommunity nicht mithalten. Über das letzte Jahr hinweg haben wir beobachtet, wie Bedrohungen Geräte in jedem Teil einer Organisation ausnutzten – von herkömmlichen IT-Geräten bis hin zu OT-Steuergeräten oder einfachen IoT-Sensoren. Die Sicherheit von IT-Geräten hat sich in den letzten Jahren gefestigt, aber die Sicherheit von IoT- und OT-Geräten hat nicht damit Schritt halten können. Akteure etablieren über solche Geräte Zugriff auf Netzwerke und ermöglichen laterale Bewegung oder stören die OT-Abläufe der Organisation. Wir haben Angriffe auf Stromnetze erlebt, Ransomware-Angriffe, die OT-Abläufe stören, IoT-Router, die für die Steigerung der Persistenz missbraucht werden, und Angriffe auf Schwachstellen in Firmware.

Die Verbreitung von IoT- und OT-Schwachstellen stellt für alle Organisationen eine Herausforderung dar, aber auch kritische Infrastruktur ist einem erhöhten Risiko ausgesetzt, weil die Akteure gelernt haben, dass das Ausschalten kritischer Dienstleistungen ein mächtiger Hebel ist. Der Ransomware-Angriff von 2021 auf die Colonial Pipeline Company hat gezeigt, wie Kriminelle eine kritische Dienstleistung stören können, um die Aussicht auf eine Lösegeldzahlung zu erhöhen. Und Russlands Cyberangriffe gegen die Ukraine demonstrieren, dass einige Nationalstaaten Cyberangriffe gegen kritische Infrastrukturen als akzeptable Sabotage ansehen, um ihre militärischen Ziele zu erreichen.

Es gibt jedoch einen Silberstreif am Horizont. Gesetzgeber und Netzwerkverteidiger werden aktiv, um die Cybersicherheit von kritischer Infrastruktur zu verbessern. Dazu gehören auch IoT- und OT-Geräte, auf die sie sich stützt. Gesetzgeber beschleunigen die Entwicklung von Gesetzen und Vorschriften, um öffentliches Vertrauen in die Cybersicherheit kritischer Infrastrukturen und Geräte aufzubauen.

Microsoft arbeitet mit Regierungen auf der ganzen Welt zusammen, um diese Gelegenheit dafür zu nutzen, die Cybersicherheit zu verbessern, und wir freuen uns über weitere Beteiligung. Jedoch können uneinheitliche, maßgeschneiderte oder komplexe Anforderungen auch unbeabsichtigte negative Auswirkungen haben. Beispielsweise könnte das Umleiten wichtiger Sicherheitsressourcen zum Sicherstellen von Compliance mit mehreren doppelten Zertifizierungen die Sicherheit in einigen Fällen beeinträchtigen.

Aus sicherheitstechnischer Sicht verfolgen Netzwerkverteidiger*innen mehrere Ansätze, um den IoT-/OT-Sicherheitsstatus ihrer Organisationen zu verbessern. Ein Ansatz besteht im Implementieren kontinuierlicher Überwachung von IoT- und OT-Geräten. Ein weiterer ist der sogenannte Shift-Left-Ansatz. Das heißt, dass für die IoT- und OT-Geräte selbst bessere Methoden für die Cybersicherheit angefordert und implementiert werden.
Ein dritter Ansatz besteht im Implementieren einer Sicherheitsüberwachungslösung, die sowohl IT- als auch OT-Netzwerke umfasst. Dieser ganzheitliche Ansatz bietet den deutlichen zusätzlichen Vorteil, dass er zu wichtigen organisatorischen Prozessen beiträgt, z. B. das Aufbrechen von Silos zwischen OT und IT, was die Organisation wiederum in die Lage versetzt, einen besseren Sicherheitsstatus zu erlangen und gleichzeitig die Geschäftsziele zu erfüllen.

Michal Braverman-Blumenstyk
Corporate Vice President, Chief Technology Officer, Cloud and AI Security

Regierungen handeln, um die Sicherheit und Resilienz von kritischer Infrastruktur zu verbessern

Regierungen auf der ganzen Welt entwickeln und verbessern Richtlinien für den Umgang mit dem Cybersicherheitsrisiko für kritische Infrastruktur. Viele erlassen auch Richtlinien zur Verbesserung der Gerätesicherheit. Die wachsende globale Welle politischer Initiativen schafft enorme Möglichkeiten zur Verbesserung der Cybersicherheit, bedeutet aber auch Herausforderungen für Stakeholder*innen in der gesamten Infrastruktur.

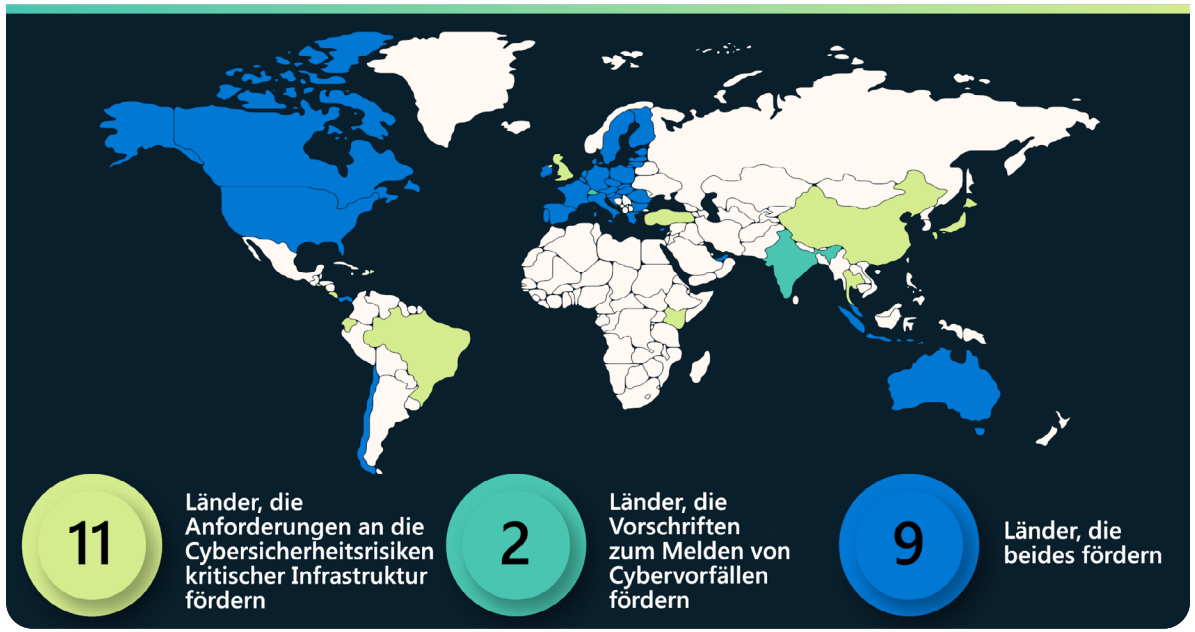
Die Entwicklung einer ganzheitlichen Vision für den Umgang mit Cyberrisiken in der kritischen Infrastruktur ist entscheidend, aber auch komplex, insbesondere angesichts des Grades der Vernetzung zwischen Technologien und globalen Lieferanten, der Bandbreite der verschiedenen Anwendungen und der damit verbundenen Risiken und der Notwendigkeit, in sowohl kurz- als auch langfristige Strategien zu investieren. Effektiv bemessene Richtlinien, die iteratives Lernen und iterative Verbesserungen fördern und weltweite sektorübergreifende Interoperabilität fördern, können dabei helfen, die Komplexität zu beherrschen und eine mehr auf Sicherheit ausgerichtete digitale Transformation zu ermöglichen. Ein fragmentierter Ansatz für die Gesetzgebung könnte jedoch zu Überschneidungen und uneinheitlichen gesetzlichen Anforderungen führen. Dies könnte sich wiederum auf Ressourcen auswirken und letztlich die Sicherheitsziele untergraben. Beispielsweise könnte eine Folge sein, dass Organisationen ihre Ressourcen von Innovations- und Sicherheitsthemen abziehen, um stark formalistisch geprägte Compliance-Aspekte zu unterstützen.

Microsoft engagiert sich für effektive Cybersicherheitsrichtlinien für kritische Infrastruktur, für ein besseres Verständnis der Herausforderungen und Chancen sowie für Initiativen, um eine Verbesserung der kollektiven Sicherheitslage zu erzielen, und geht mit Regierungen auf der ganzen Welt Partnerschaften ein.

Politische Entwicklungen beim Cybersicherheitsrisikomanagement für kritische Infrastruktur

Im letzten Jahr haben mehrere Gerichtsbarkeiten, darunter Australien, Chile, die Europäische Union (EU), Japan, Singapur, Großbritannien und die USA, branchenübergreifende oder branchenspezifische Anforderungen an Cybersicherheit entwickelt, aktualisiert oder implementiert.[1] Viele dieser Regierungen – und andere wie Indien[2] und die Schweiz[3] – haben bereits Meldepflichten für Cybersicherheitsvorfälle bei kritischer Infrastruktur und wichtigen Dienstanbietern erlassen oder arbeiten sie gerade aus.[4]

In Australien, der EU, Indonesien und den USA gab es im letzten Jahr einige nennenswerte politische Entwicklungen. Australien hat zwei Gesetze erlassen, die den Umgang mit Cybersicherheitsrisiken für branchenübergreifende kritische Infrastruktur erleichtern sollen. Unter anderem legen die Gesetze neue Bereiche kritischer Infrastruktur fest, verlangen die Entwicklung eines Risikomanagementplans, schreiben das Melden von Cybersicherheitsvorfällen vor und ermächtigen die Regierung zu intervenieren, wenn sie feststellt, dass ein Betreiber von kritischer Infrastruktur nicht bereit oder nicht in der Lage ist, angemessen auf einen Vorfall zu reagieren.



Die EU arbeitete an einer neuen Fassung ihrer NIS-Richtlinie von 2016. Sie bietet EU-Mitgliedstaaten einen Rahmen für die Regulierung technologischer Dienste und Produkte, die als lebenswichtig für deren Wirtschaft und das Funktionieren der Gesellschaft angesehen werden. Der Entwurf für NIS 2 umfasst Details, die eine neue Kategorie von kritischer digitaler Infrastruktur etablieren, die Anforderungen an Meldungen von Cybervorfällen erhöhen und zusätzliche Anforderungen an Cybersicherheitsrisikomanagement stellen würden. Die EU hat auch einen Entwurf für eine Neufassung ihrer DORA-Richtlinie (Digital Operational Resilience Act) entwickelt. Darin enthalten sind neue Anforderungen für Technologien zur Datenkommunikation, die im Finanzdienstleistungssektor eingesetzt werden.

Im Mai verabschiedete Indonesien eine Präsidialverordnung zum Schutz der vitalen Informationsinfrastruktur („IIV"), die im Mai 2024 in Kraft treten wird und unter anderem Bereiche wie Energie, Verkehr, Finanzdienstleistungen und Gesundheitswesen abdeckt. Indonesien will mit dieser Verordnung die Kontinuität bei der Implementierung von IIV sicherstellen, Cyberangriffe verhindern und die Vorbereitung auf die Bewältigung von Cybervorfällen verbessern. IIV-Anbieter werden für sicheren und zuverlässigen Schutz verantwortlich sein sowie für die Implementierung eines effektiven Cyberrisikomanagements und für das Melden von Cyberrisikoergebnissen an die entsprechenden Behörden. Die Verordnung umfasst die Pflicht, Cybervorfälle innerhalb von 24 Stunden zu melden.

Regierungen handeln, um die Sicherheit und Resilienz von kritischer Infrastruktur zu verbessern

Fortsetzung

Der US-Kongress verabschiedete ein Gesetz, das die Cyber and Infrastructure Security Agency (CISA) ermächtigt, Verordnungen über Meldepflichten für Cybervorfälle bei kritischer Infrastruktur zu erlassen, und die Transportation Security Administration (TSA) hat neue branchenspezifische Cybervorschriften im Transportsektor verordnet. In Reaktion auf den Ransomware-Angriff auf die Colonial Pipeline Company erließ die TSA 2021 zwei Sicherheitsrichtlinien für Betreiber von Pipelines für gefährliche Flüssigkeiten und Erdgas:

- Die erste Verordnung verlangt von den Betreibern, eine(n) Cybersicherheitskoordinator*in zu benennen, Cybervorfälle innerhalb von zwölf Stunden zu melden und eine Schwachstellenbewertung ihrer Systeme durchzuführen.
- Die zweite Verordnung, die die TSA 2022 noch einmal überarbeitete, forderte die Betreiber auf, spezifische Schutzmaßnahmen gegen Ransomware-Angriffe und andere bekannte Bedrohungen für IT- und OT-Systeme zu implementieren, binnen 30 Tagen einen Cybersicherheitsnotfall- und -reaktionsplan zu entwickeln und zu implementieren und sich jährlichen Prüfungen des Aufbaus ihrer Cybersicherheitsarchitektur zu unterziehen.

Auf der Grundlage der Verordnungen für Pipelines gab die TSA später im Jahr 2021 zwei zusätzliche Sicherheitsverordnungen heraus, die Cybersicherheitsanforderungen an Betreiber von Güter- und Personenschienenverkehr oder Schienennahverkehrssystemen stellten. Die Verordnungen schrieben vor, dass die darunter fallenden Betreiber einen Cybersicherheitskoordinator benennen, Cybersicherheitsvorfälle binnen 24 Stunden melden und einen Reaktionsplan für Cybersicherheitsvorfälle entwickeln und implementieren und eine Cybersicherheitsschwachstellenbewertung ihrer Systeme durchführen. Gleichzeitig verkündete die TSA, dass sie außerdem ihre Sicherheitsprogramme für die Luftfahrt aktualisiert hat, die die Betreiber von Flughäfen und Fluggesellschaften jetzt zur Implementierung der ersten zwei Bestimmungen verpflichtet: das Benennen eines Koordinators und das Melden von Vorfällen innerhalb von 24 Stunden.

Politische Entwicklungen bei der Sicherheit von IoT- und OT-Geräten

In Dutzenden von Ländern sind die Regierungen damit beschäftigt, Anforderungen für die Cybersicherheit von Produkten und Diensten der Informations- und Kommunikationstechnologie (IKT) auf Weg zu bringen. Dies erstreckt sich auch auf IoT- und OT-Geräte. Im Zusammenhang mit IKT-Produkten und -Diensten bestehen die größten Bedenken bei der Sicherheit der Softwarelieferkette sowie bei IoT-Sicherheit.

- Die Europäischen Kommission hat den Cyber Resilience Act vorgeschlagen. Er würde Cyberanforderungen für eigenständige Software und vernetzte Geräte sowie für die zugehörigen Dienste festlegen.[5] Relevante Verfahren für Softwareanbieter umfassen die Anwendung eines sicheren Softwareentwicklungszyklus[6] und die Bereitstellung einer Softwarestückliste.[7] Neue Sicherheitsanforderungen gelten für vernetzte Geräte, und alle Hersteller hätten die Pflicht, für veröffentlichte Produkte eine koordinierte Offenlegung von Sicherheitslücken durchzuführen.[8]

Die Gesetzgeber haben auch die fortgesetzte Verbreitung von IoT-Geräten und vernetzten OT-Geräten im Blick.

- In Großbritannien sieht der Entwurf für die Security and Telecommunications Infrastructure Bill vor, Hersteller von vernetzten Produkten für Verbraucher, wie z. B. Smart-TVs, dazu zu verpflichten, keine standardmäßigen Kennwörter mehr zu verwenden, die ein leichtes Ziel für Cyberkriminelle darstellen, eine Richtlinie für die Offenlegung von Schwachstellen zu etablieren (z. B. eine Methode zum Erhalten von Mitteilungen über Sicherheitsmängel) und Transparenz zu schaffen in Bezug auf die Mindestzeitspanne, über die sie Sicherheitsupdates bereitstellen werden.[9]
- In der EU werden neue Sicherheitsstandards oder -anforderungen über mehrere gesetzgeberische Instrumente implementiert. Dazu gehört ein delegierter Rechtsakt zur Richtlinie zu Funkanlagen, die sich an drahtlose Geräte richtet und zum Ziel hat, die Netzwerkresilienz zu verbessern, die Privatsphäre von Kund*innen zu schützen und das Risiko monetären Betrugs zu reduzieren.[10] Darüber könnte auch die Anwendung eines Programms zur Cloudzertifizierung[11] vorgeschrieben werden, wie es derzeit als Ergebnis des EU Cybersecurity Act von 2019[12] in Planung ist.

Die Notwendigkeit von Konsistenz

In vielen Fällen wird die ganze Bandbreite der Regionen, Branchen, Technologien und Bereiche des operativen Risikos umspannenden Aktivitäten gleichzeitig verfolgt, was zu potenziellen Überschneidungen oder Inkonsistenzen bei Umfang, Anforderungen und Komplexität für Organisationen führt, die sich eindeutige Anweisungen wünschen oder Compliance demonstrieren wollen. Ohne eine allgemein akzeptierte Definition von IoT ist der Umfang eine besondere Herausforderung für die Regulierung von IoT- und OT-Geräten. Die obigen Beispiele beziehen sich möglicherweise auf „vernetzte Produkte und entsprechende Dienste“, „vernetzte Produkte für Verbraucher*innen“ und „drahtlose Geräte“. Gleichzeitig wünschen sich viele Regierungen robustere Bewertungsverfahren, um besser zu verstehen, ob und wie Organisationen und Produkte aktuelle, geplante und zukünftige Anforderungen einhalten. Wenn sich diese Trends vereinen, führt dies zu mehr Komplexität. Es ist ermutigend, dass die Fragen, die bei Beratungen zum EU Cyber Resilience Act gestellt wurden, darauf eingingen, wie neue Regulierungen möglicherweise mit vorhandenen Cybersicherheitsvorschriften zusammenwirken könnten. Die zeigt den Willen, widersprüchliche Verordnungen zur Cybersicherheit zu vermeiden.

Iterative Ansätze, die risikobasiert und ergebnis- oder prozessorientiert sind (im Vergleich zur implementierungsspezifischen Ansätzen), könnten die Cybersicherheit stärken und für kontinuierliche Verbesserungen sorgen. Auf ähnliche Weise könnte ein Fokus auf das Schaffen von regions-, sektor- und geltungsbereichsübergreifender Kompatibilität die Cybersicherheit konsistent über vernetzte globale Lieferketten hinweg steigern.

Regierungen handeln, um die Sicherheit und Resilienz von kritischer Infrastruktur zu verbessern

Fortsetzung

Es sind zunehmend komplexe regions-, sektor- und themenbereichsübergreifende Cybersicherheitsrichtlinien für kritische Infrastruktur in Entwicklung. Diese Aktivität bietet große Chancen und erhebliche Herausforderungen. Die Vorgehensweise von Regierungen wird entscheidend sein für die Zukunft der digitalen Transformation und die Sicherheit in der gesamten Infrastruktur.

Beschleunigung der infrastrukturweiten Investitionen in die Sicherheit der Softwarelieferkette und der Zero Trust-Architektur

Die US Executive Order (EO) 14028 zur Verbesserung der Cybersicherheit war ein Katalysator, der die laufenden Initiativen von Microsoft für Investitionen in die Sicherheit unserer eigenen und der infrastrukturweiten Lieferkette sowie zur Befähigung unserer Kund*innen zum Einhalten von Zero Trust-Zielen unterstützte.

Wir sind seit langem der Auffassung, dass ein Verbessern der Softwarelieferkette einen Austausch von Erfahrungen und bewährten Methoden erfordert. Das beginnt mit unserer Veröffentlichung des Microsoft Security Development Lifecycle vor 15 Jahren.

Darüber hinaus arbeiten wir eng mit dem National Cybersecurity Center of Excellence zusammen, um Ansätze zur Zero Trust-Architektur zu demonstrieren, die sowohl auf On-Premises- als auch auf Cloud-Technologie angewendet werden, und um neue Produktfunktionen zu entwickeln, darunter z. B. die Fähigkeit, eine Phishing-resistente Authentifizierung für Hybrid- und Multi-Cloud-Umgebungen zu erzwingen.

Heute gehen wir über die Anforderungen der EO hinaus, um Konformität mit den Sicherheitsanforderungen der Softwarelieferkette zu demonstrieren und auf zwei verschiedenen Wegen Softwarestücklisten (Software Bill of Materials, SBOM) bereitzustellen:

1. Erstens stellen wir eine Open Source-Version unseres SBOM-Generatortools zur Verfügung, das wir so entwickelt haben, dass es sich leicht in CI-/CD-Pipelines integrieren lässt, die Windows-, Linux-, Mac-, iOS- und Android-Plattformen unterstützen.[13]
2. Zweitens leisten wir einen Beitrag zur Entwicklung von Branchenstandards für Lieferkettenintegrität, Transparenz und Vertrauen (Supply Chain Integrity, Transparency, and Trust, SCITT). Dies ermöglicht einen automatisierten Austausch von überprüfbaren Lieferkettendaten, einschließlich Artefakten, die die Konformität mit den Anforderungen nachweisen, welche sich aus den Anweisungen der EO für die Softwarelieferkette ergeben.

Umsetzbare Insights

1. Multilaterale Institutionen müssen neu gedacht werden, um die drängenden Herausforderungen nationalstaatlicher Cyberattacken zu bewältigen.
2. Entwickeln Sie Cybersicherheitsrichtlinien, die über alle Regionen, Sektoren und Themenbereiche hinweg konsistent und kompatibel sind.

Links zu weiteren Informationen

- Continued investments in supply chain security in support of the cybersecurity Executive Order | Microsoft Tech Community
- US Government sets forth Zero Trust architecture strategy and requirements | Microsoft Security Blog
- CYBER EO | Microsoft Federal
- Supply Chain Integrity, Transparency, and Trust | github.com
- Implementing a Zero Trust Architecture | NCCoE (nist.gov)

IoT und OT im Visier: Trends und Angriffe

Eine zunehmend vernetzte digitale Welt bedeutet, dass schnell immer mehr Geräte online gehen, mit größeren Systemen kommunizieren, Daten sammeln und ehemals verborgene Bereiche sichtbar machen. Dies birgt Chancen für Organisationen, aber auch für kriminelle Akteure, weil das Geschäft mit Cyberkriminalität einerseits zu einer milliardenschweren Branche und andererseits zum Risiko wird.

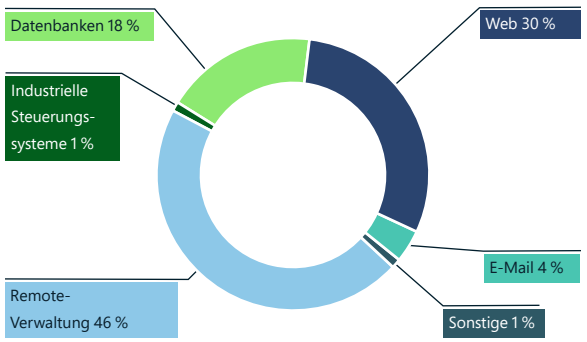
IoT-Geräte, darunter alles von Druckern und Webcams über Klimageräte bis hin zu Steuerungssystemen für Gebäudezugänge, stellen einzigartige Sicherheitsrisiken für Einzelpersonen, Organisationen und Netzwerke dar. Obwohl sie für den Geschäftsbetrieb vieler Unternehmen überlebenswichtig sind, können sie auch schnell zu einem Haftungs- und Sicherheitsrisiko werden. Die schnelle Einführung von IoT-Lösungen in fast allen Branchen hat die Zahl der Angriffsvektoren und das Expositionsrisiko von Organisationen erhöht.

Malware-as-a-Service hat sich auf groß angelegte Operationen gegen zivile Infrastruktur und Versorgungsunternehmen (einschließlich Krankenhäusern, Öl- und Gasversorgern, Stromnetzen, Verkehrsbetrieben und anderer kritischer Infrastruktur) sowie Unternehmensnetzwerke verlagert. Akteure müssen erheblichen Forschungsaufwand betreiben, um die Konfiguration von Betriebsumgebungen und eingebetteten IoT- und OT-Geräten zu ermitteln und auszunutzen.

IoT-Geräte stellen einzigartige Sicherheitsrisiken dar, weil sie im Netzwerk sowohl als Einstiegs- als auch Ausgangspunkte fungieren können. Millionen von IoT-Geräten sind ungepatcht oder exponiert.

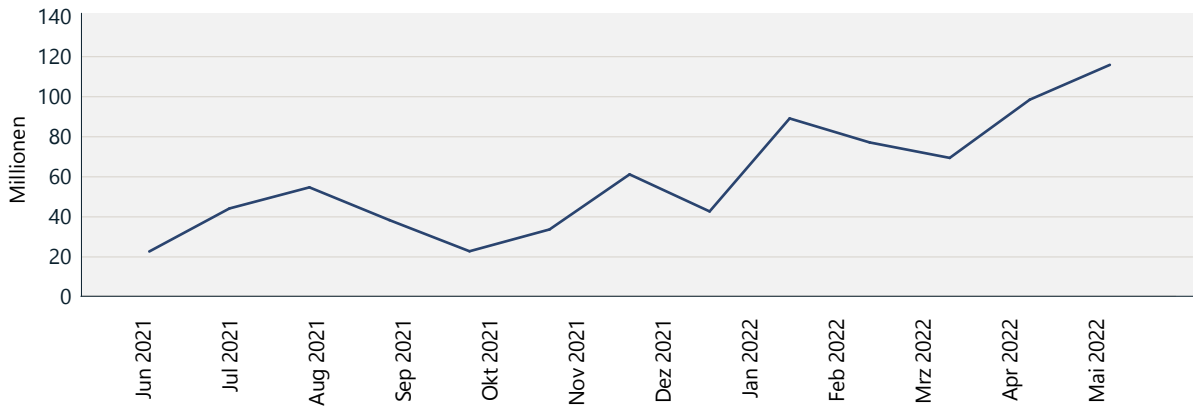
Exponierte Geräte lassen sich über Suchtools im Internet finden. Dazu werden die Dienste über ein Belauschen offener Netzwerkports identifiziert. Diese Ports werden häufig für die Remote-Verwaltung von Geräten verwendet. Wenn sie nicht richtig abgesichert sind, kann ein exponiertes Gerät als Ausgangspunkt für den Zugriff auf eine andere Ebene des Unternehmensnetzwerk verwendet werden, weil unautorisierte Benutzer*innen remote auf die Ports zugreifen können. Wir haben beobachtet, wie verschiedene Akteure versucht haben, Schwachstellen in exponierten Internetgeräten auszunutzen. Dabei reichte die Spanne von Kameras über Router bis hin zu Thermostaten. Allerdings bleiben trotz des Risikos Millionen von Geräten ungepatcht oder ungeschützt.

Zusammenfassung der Angriffstypen auf IoT/OT



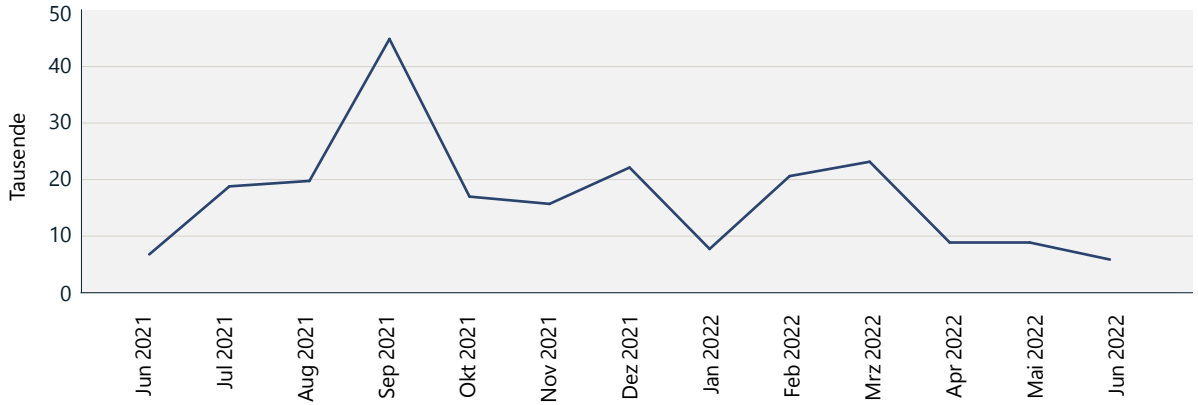
Über das MSTIC-Sensornetzwerk beobachtete Angriffstypen. Am häufigsten waren Angriffe auf Remote-Verwaltungsgeräte, Angriffe über das Web und Angriffe auf Datenbanken (Brute-Force oder Exploits).

Angriffe auf Remote-Verwaltungsgeräte



Angriffe auf Remote-Verwaltungsports im Laufe der Zeit, wie über das MSTIC-Sensornetzwerk beobachtet.

Webangriffe gegen IoT und OT



Das Volumen von Webangriffen, wie über das MSTIC-Sensornetzwerk beobachtet. Da die Anzahl der direkt mit dem Web verbundenen Geräte weiterhin abnimmt, können Angreifer letzten Endes nicht mehr so leicht danach suchen.

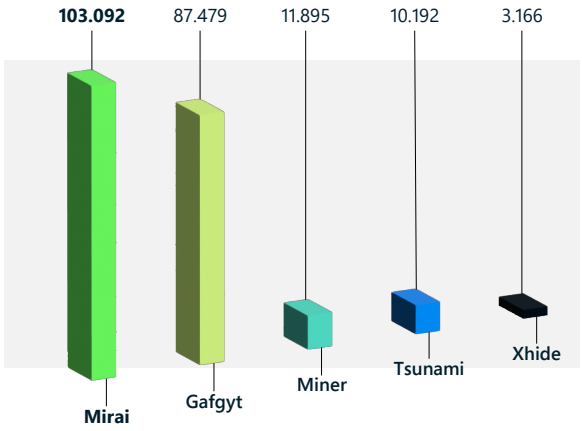
IoT und OT im Visier: Trends und Angriffe

Fortsetzung

Überarbeitetes Schadsoftware-Dienstprogramm

So wie sich cyberkriminelle Gruppen weiterentwickelt haben, gilt dies auch für deren Bereitstellung von Schadsoftware und die Auswahl der Ziele. Im letzten Jahr haben wir Angriffe auf gängige IoT-Protokolle wie Telnet beobachtet, die in einigen Fällen mit bis zu 60 % deutlich gesunken sind. Gleichzeitig wurden Botnets von cyberkriminellen Gruppen und nationalstaatlichen Akteuren umfunktioniert. Die Persistenz von Schadsoftware wie Mirai zeigt, wie modular diese Angriffe aufgebaut sind und wie sehr sich vorhandene Bedrohungen anpassen können.

Häufigste beobachtete IoT-Schadsoftware in freier Wildbahn



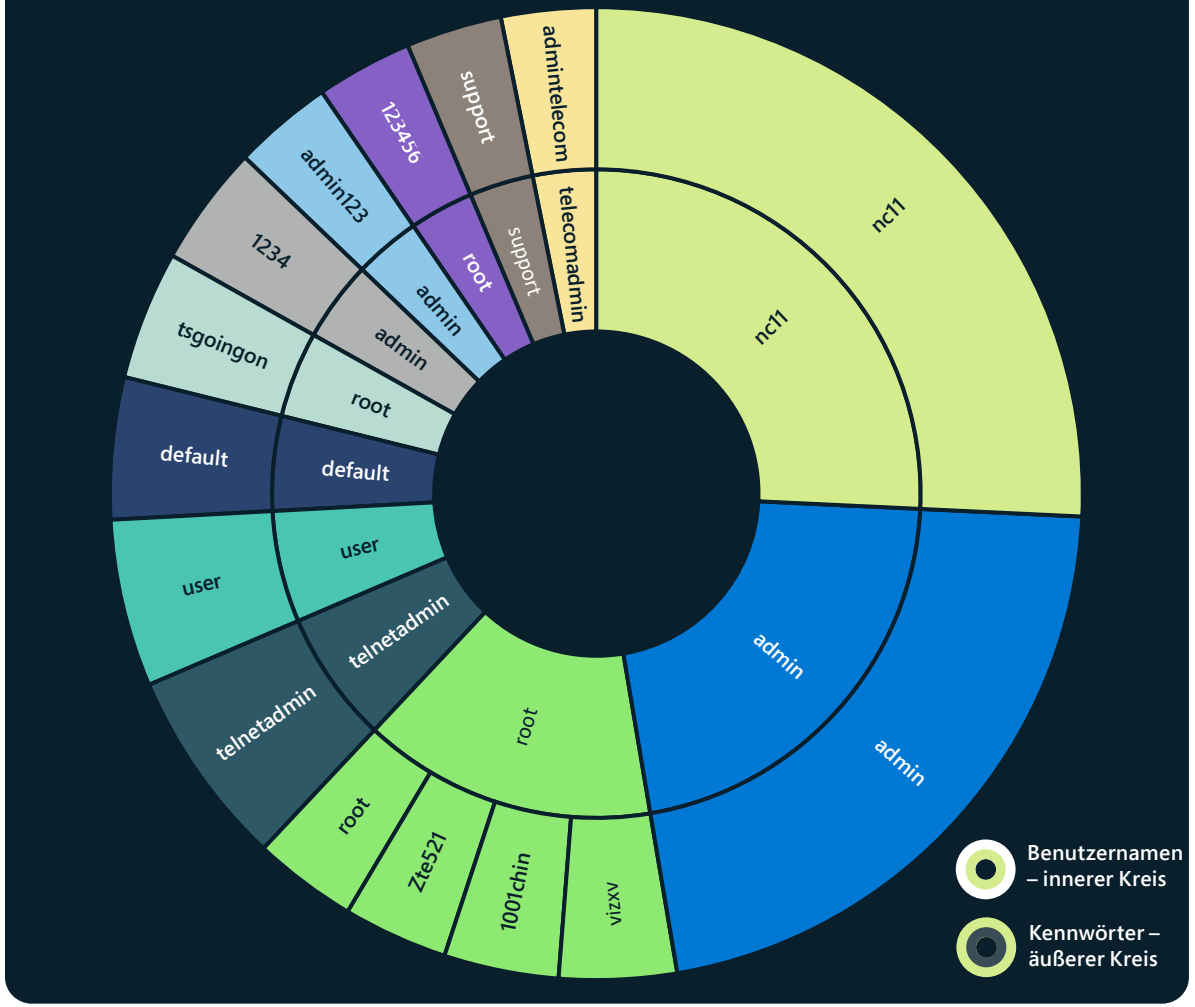
Mirai hat sich weiterentwickelt und mittlerweile eine Vielzahl von Geräten infiziert, darunter Internetprotokollkameras, digitale Videorecorder für Sicherheitskameras und Router. Der Angriffsvektor hat die veralteten Sicherheitskontrollen umgangen und stellt ein Risiko für Endpunkte innerhalb des Netzwerks dar, indem er zusätzliche Schwachstellen ausnutzt und sich lateral bewegt. Mirai wurde mehrmals neu gestaltet, wobei sich die Varianten an verschiedene Architekturen anpassen und sowohl bekannte als auch Zero-Day-Schwachstellen für die Kompromittierung neuer Angriffsvektoren ausnutzen.

Die Nutzung von Mirai stieg im letzten Jahr sowohl bei 32- als auch bei 64-Bit x86-CPU-Architekturen an, und die Schadsoftware erhielt neue Funktionen, die schnell von Nationalstaaten und kriminellen Gruppen übernommen wurden. Nationalstaatliche Angriffe nutzen nun neue Varianten vorhandener Botnets in DDoS-Angriffen auf ausländische Gegner.

Weil die Einnahmen aus Angriffen gegen IoT-Geräte 2022 zurückgingen, haben wir beobachtet, wie mehrere Gruppen von Akteuren Schwachstellen ausnutzten – z B. Log4j und Spring4Shell –, um eine bösartige Nutzlast an Geräte wie Server zu senden, sie zu infizieren und sie für große Botnets zu rekrutieren, die DDoS-Angriffe durchführen. Das überarbeitete Dienstprogramm von Schadsoftware, die auf Schwachstellen von IoT-Geräten abzielt, hat gravierende Auswirkungen auf Organisationen und Nationen, weil laterale Bewegung Hintertüren für weitere Nutzlasten sowie andere Geräte in Netzwerken offenlegen kann.

Viele Protokolle von industriellen Steuerungssystemen werden nicht überwacht und sind daher anfällig für OT-spezifische Angriffe. Dies kann ein erhöhtes Risiko für kritische Infrastruktur bedeuten.

Relative Prävalenz von Paaren aus Benutzername/Kennwort, die bei IoT-/OT-Geräten in 45 Tagen mit Sensorsignalen aufgetreten sind



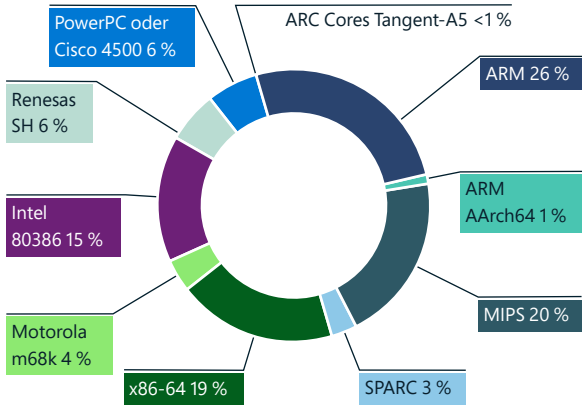
Die Verwendung gängiger Paare aus Benutzername und Kennwort erhöht das Risiko einer Kompromittierung. In einer Stichprobe mit über 39 Millionen IoT- und OT-Geräten verwendeten etwa 20 % identische Benutzernamen und Kennwörter.

IoT und OT im Visier: Trends und Angriffe

Fortsetzung

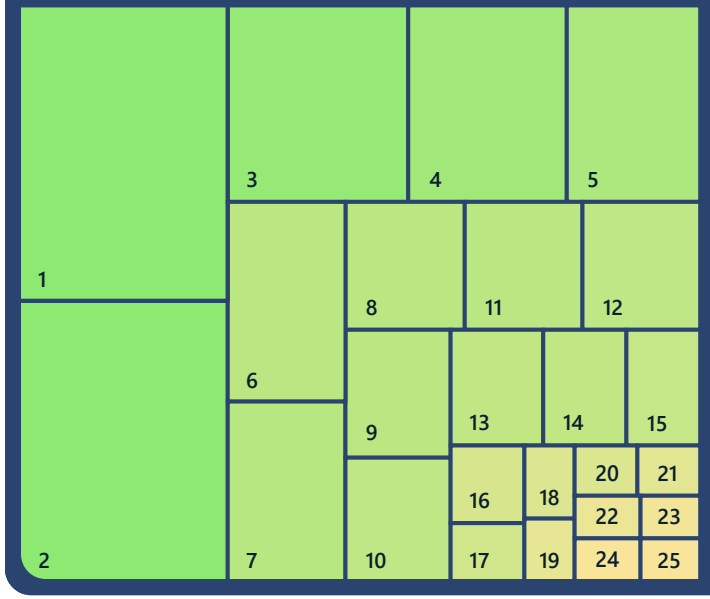
Während schwache Konfigurationen und standardmäßige Anmeldeinformationen weiterhin ein Risiko für Netzwerke darstellen, hat Microsoft viele webbasierte Exploits beobachtet, die HTTP nutzen. Wir haben diese Zunahme von Angriffen auf webbasierte Dienste mithilfe von alten Botnets beobachtet. In der Zwischenzeit gab es einen Rückgang bei der Anzahl offener Telnet-Ports im Internet. Dies ist ein positives Zeichen für die Netzwerksicherheit, weil Botnets, die in der Vergangenheit ein Risiko für Geräte darstellten, an Relevanz verlieren. Trotz dieses Rückgangs von offenen Telnet-Ports haben wir weiterhin persistente Botnets in Sensornetzwerken beobachtet.

Verteilung von IoT-Schadsoftware nach CPU-Architektur



Microsoft hat beobachtet, das auf ARM ausgeführte IoT-Geräte am häufigsten von Schadsoftware angegriffen werden, gefolgt von MIPS, X86-64 und Intel 80386 CPU.

Verbreitung von Protokollen industrieller Steuerungssysteme



1. EtherNet/IP
2. MODBUS
3. BACNet
4. Siemens S7
5. Profinet Real-Time
6. Profinet DCP
7. Siemens S7 Plus
8. CodeSys
9. Siemens WinCC Agent
10. EtherNet/IP O/O
11. Honeywell Control Data Access
12. MMS
13. IEC-60870
14. Honeywell FDA Diagnostics
15. Suitelink
16. DeltaV
17. GSM
18. DNP3
19. AMS
20. SRTP
21. TwinCat
22. Emerson Roc
23. Bently Nevada
24. Mitsubishi MELSEC
25. TriStation Tricon

Schwachstellen in Protokollen industrieller Steuerungssysteme

Wir haben uns OT-Daten aus unseren cloudvernetzten Sensoren angesehen, aus denen die gängigsten Protokolle für industrielle Steuerungssysteme (Industrial Control Systems, ICS) hervorgingen. Diese Protokolle geben Einblicke in die Art dieser Geräte und ihre Angriffsfläche. Dies ist besonders wichtig für die Sicherheit kritischer Infrastrukturen. Einige wichtige Erkenntnisse sind:

1. Die meisten der aufgeführten Protokolle sind proprietär, sodass standardmäßige IT-Überwachungstools keine ausreichende Sicherheitstransparenz für diese Geräte und Protokolle bieten. Infolgedessen bleiben Netzwerke unüberwacht und sind daher anfälliger für OT-spezifische Angriffe.
2. Es gibt eine Vielzahl von herstellerspezifischen Protokollen. Dies bedeutet, dass anbieterspezifische Sicherheitslösungen nicht in der Lage sind, das gesamte Netzwerk angemessen abzudecken. Microsoft gibt einer anbieterunabhängigen Herangehensweise den Vorzug, um eine Sicherheitsabdeckung für die Vielzahl der verschiedenen Geräte zu bieten.
3. Organisationen sollten sicherstellen, dass diese Protokolle nicht direkt über ihre Netzwerke aus dem Internet verfügbar sind. Aufgrund von Schwachstellen und der inhärenten Unsicherheit dieser Protokolle kann eine solche Exposition ein großes Sicherheitsrisiko darstellen.

Das beharrliche Fortbestehen von Schadsoftware wie Mirai beruht auf der Entwicklung neuer Funktionen sowie der Tatsache, dass sie von cyberkriminellen Gruppen und nationalstaatlichen Akteuren genutzt wird. Dabei wird für DDoS-Angriffe auf ausländische Gegner auf neue Varianten vorhandener Botnets zurückgegriffen.

Umsetzbare Insights

1. Stellen Sie sicher, dass die Geräte ausreichend geschützt sind, indem Sie Patches anwenden und Standardkennwörter sowie standardmäßige SSH-Ports ändern.
2. Reduzieren Sie die Angriffsfläche, indem Sie unnötige Internetverbindungen und offene Ports beseitigen, den Remote-Zugriff durch das Blockieren von Ports einschränken, den Remote-Zugriff verweigern und VPN-Dienste nutzen.
3. Verwenden Sie eine IoT-/OT-fähige NDR-Lösung (Network Detection and Response) sowie eine SIEM-/SOAR-Lösung zur Überwachung von Geräten auf anormales oder unautorisiertes Verhalten, z. B. die Kommunikation mit unbekannten Hosts.
4. Segmentieren Sie Netzwerke, um die Fähigkeit von Angreifern zu lateraler Bewegung und zur Kompromittierung von Ressourcen nach dem ersten Eindringen zu begrenzen. IoT-Geräte und OT-Netzwerke sollten durch Firewalls von den IT-Netzwerken des Unternehmens isoliert werden.
5. Stellen Sie sicher, dass ICS-Protokolle nicht direkt im Internet exponiert sind.

Hackerangriffe auf Lieferketten und Firmware

Fast jedes Gerät mit Internetverbindung besitzt eine Firmware, die in die Hardware oder Platine des Geräts eingebettet ist. In den letzten Jahren haben wir eine Zunahme der Angriffe auf Firmware beobachtet, über die dann verheerende Angriffe gestartet wurden. Weil zu vermuten ist, dass Firmware ein lohnendes Ziel für Akteure bleiben wird, müssen sich Organisationen gegen Hackerangriffe auf Firmware wappnen.

Die Firmware steuert die primären Funktionen eines Geräts, z. B. die Verbindung mit einem Netzwerk oder das Speichern von Daten. Firmware findet sich in Routern, Kameras, Fernsehern und anderen Geräten, die in Unternehmen verwendet werden (IoT), sowie auch in industriellen Steuerungsanlagen (OT), die in kritischer Infrastruktur zur Anwendung kommen. Früher wurde Firmware mit ungesichertem Code geschrieben. Dies erzeugte erhebliche Schwachstellen, die für die Übernahme des Geräts oder zum Einschleusen bösartigen Codes in die Firmware ausgenutzt werden konnten.

In Lieferketten ist dieses Risiko noch größer. Die meisten Geräte werden mit Software- und Hardwarekomponenten von zahlreichen verschiedenen Herstellern sowie aus Open Source-Bibliotheken entwickelt. In vielen Fällen haben die Betreiber der Geräte keinen Einblick in die Hardware- und Softwarestücklisten (H/SBOM), um das Risiko für die Geräte in der Lieferkette einschätzen zu können. Im Juni 2020 wurden Sicherheitslücken in einem von vielen unterschiedlichen Herstellern verwendeten Netzwerk-Stack offengelegt, die Hunderte Millionen von Geräten in Privathaushalten, aber auch in Industrieanlagen betrafen.[14] In einigen Fällen war zudem das Branding des Netzwerk-Stacks von anderen Herstellern verändert worden, und es gab keine Anzeichen, dass ein Gerät anfällig war. Wir sehen eine wachsende Bedrohung durch böswillige Akteure, die diese Software- und Hardwarelieferkette aus IoT-/OT-Geräten anvisieren, um Unternehmen zu kompromittieren.

Der Prozess der Firmwareaktualisierung ist von Gerät zu Gerät unterschiedlich, und die Komplexität sowie die logistische Herausforderung bei der Durchführung der Aktualisierung wirkt sich negativ auf die Aktualisierungshäufigkeit aus. Es lässt sich nicht immer feststellen, ob ein Gerät die neueste Firmware ausführt. Dies erschwert den Sicherheitsexpert*innen die Überwachung und auch die Gewährleistung eines angemessenen Sicherheitsstatus für ihre IoT- und OT-Geräte. Darüber hinaus verfügen einige Geräte über Firmware, die nicht kryptografisch signiert ist. Daher können sie ohne Bestätigung durch die Benutzer*innen aktualisiert werden. Die Schwachstellen machen die Geräte noch anfälliger für Lieferkettenangriffe in der gesamten Produktions- und Vertriebskette.

Um diese Bedrohungen zu bewältigen, tätigt Microsoft erhebliche Investitionen in die Sicherheit und Integrität der Firmware, um die verschiedenen Phasen der Lieferkette abzubilden, und in Verfahren, über die sich bestätigen lässt, dass sie am Beginn oder während ihres Lebenszyklus nicht manipuliert wurde. Auf diese Weise können wir die Vertrauensstellung in jedem Segment der Pipeline validieren und für jede Komponente, die wir an unsere Kund*innen versenden, eine zertifizierte und nachweisbare lückenlose Überwachungskette bereitstellen. Zusammen mit unseren Partnern arbeiten wir daran, alle Geräte im Unternehmens- und OT-Netzwerk mit dieser Chip-to-Cloud-Sicherheit zu versorgen.

„IKT-Infrastrukturanbieter werden zunehmend zu Zielen, weil sich ein Angriff über sie replizieren und entsprechend weit verbreiten lässt. Gleichzeitig wird auch die Latte durch globale Gesetzgebung, Regulierung und Kundenanforderungen in Bezug auf die Sicherheit und Resilienz der Lieferkette immer höher gelegt, allerdings unterscheiden sich diese Erwartungen teils erheblich voneinander.

Die Lösung besteht in einer Partnerschaft. Gemeinsam mit Lieferanten und staatlichen Einrichtungen weltweit hat Microsoft sich auf die Fahnen geschrieben, das Thema Sicherheit in unserer gesamten Lieferketteninfrastruktur anzugehen und die Anforderungen von Kunden und Regulierungsbehörden gleichermaßen zu übertreffen. Um dies zu erreichen, verfolgen wir einen umfassenden Ansatz bei Sicherheit und operativer Resilienz für die gesamte Lieferkette.

Die Steigerung der Firmware-Integrität vom Design bis zum Gerätebetrieb ist der Schlüssel zu unserem gemeinschaftlichen Ansatz. Das Gewährleisten der SDL-Prozesse von Lieferanten und eine Vertrauensstellung für Hardwareinnovationen sind Beispiele dafür, wie wir Lieferkettenintegrität „einbauen“ können.

Unsere Community setzt auf gemeinsame Forschung und Entwicklung. Dies umfasst etwa neue Techniken zum Manipulationsschutz und kryptografische Mechanismen sowie fortlaufende Überwachung und Erkennung von Anomalien. Gemeinsam machen wir Fortschritte dabei, die Attraktivität der Lieferkette als Angriffsfläche zu minimieren.“

Edna Conway,
Vice President, Security & Risk Officer,
Cloud Infrastructure

Firmwareschwachstellen im Schlaglicht

Angreifer nutzen zunehmend Schwachstellen in der Firmware von IoT-Geräten, um Unternehmensnetzwerke zu infiltrieren. Im Gegensatz zu herkömmlichen IT-Endpunkten, die XDR-Agents zum Finden von Schwachstellen verwenden, gestaltet sich die Erkennung von Schwachstellen bei IoT-/OT-Geräten viel schwieriger.

Eine aktuelle Umfrage von Microsoft und dem Ponemon Institute beleuchtet sowohl die Chancen als auch die Sicherheitsherausforderungen von IoT-Geräten in einem Unternehmen.[15] Während 68 % der Befragten der Meinung sind, dass die Einführung von IoT/OT für ihre strategische digitale Transformation von entscheidender Bedeutung ist, geben 60 % an, dass Sicherheit einer der am wenigsten gesicherten Aspekte in der IT-/OT-Infrastruktur ist.

Ein Beispiel für Angreifer, die Sicherheitslücken in der Firmware von IoT-Geräten nutzen, ist der Trickbot-Trojaner, der Standardkennwörter und Schwachstellen in MikroTik-Routern[16] ausnutzt, um die Verteidigungssysteme von Unternehmen zu umgehen. Die grundlegende Herausforderung bei der Firmware von IoT-Geräten besteht in der mangelnden Transparenz des Sicherheitsstatus und der Schwachstellen von Geräten.

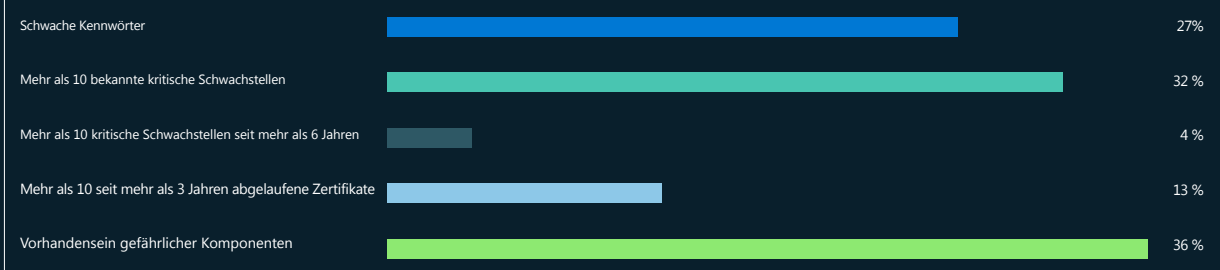
Es gibt zwar Lösungen für die Entwicklung sicherer Geräte, aber es sind bereits Milliarden von Geräten auf dem Markt und in den Unternehmen vorhanden. Diese Geräte werden als Brownfield-Geräte bezeichnet. 2021 hat Microsoft Refirm Labs gekauft, um die Sicherheit von Brownfield-Geräten zu beleuchten und die Gerätehersteller in die Lage zu versetzen, die Sicherheit ihrer Produkte zu verbessern. Refirm Labs analysiert das binäre Firmware-Image eines Geräts und erstellt einen detaillierten Bericht über potenzielle Sicherheitsschwächen.[17] Diese Technologie wird in eine zukünftige Version von Microsoft Defender for IoT integriert sein.

Im letzten Jahr haben wir aggregierte Ergebnisse der jeweils von unseren Kund*innen gescannten individuellen Firmware untersucht. Auch wenn nicht alle entdeckten Schwächen ausgenutzt werden können, unterstreichen sie dennoch die grundlegende Herausforderung, vor die uns die Sicherheit von Geräte-Firmware stellt.

Beachten Sie, dass die Arten von Schwachstellen, die in IoT-/OT-Geräten vorhanden sind, an herkömmlichen Windows- oder Linux-Endpunkten niemals akzeptabel wären.

- Schwache Kennwörter: 27 % der gescannten Firmware-Images enthielten Konten mit Kennwörtern, die mit schwachen Algorithmen (MD5/DES) kodiert wurden. Diese lassen sich von Angreifern leicht knacken.

Sicherheitsschwachstellen in analysierten Firmware-Images



- Bekannte Schwachstellen: Wie andere Systeme greift auch die Firmware von IoT-/OT-Geräten in großem Umfang auf Open Source-Bibliotheken zurück. Allerdings werden Geräte häufig mit veralteten Versionen dieser Komponenten ausgeliefert. In unserer Analyse enthielten 32 % der Images mindestens zehn bekannte Schwachstellen (CVEs), die als „kritisch“ eingestuft sind (9,0 oder höher). Vier Prozent enthielten mindestens zehn kritische Schwachstellen, die älter als sechs Jahre waren.
- Abgelaufene Zertifikate: Mit Zertifikaten werden Verbindungen und Identitäten authentifiziert und vertrauliche Daten geschützt, doch 13 % der analysierten Images enthielten mindestens zehn Zertifikate, die seit mehr als drei Jahren abgelaufen waren.
- Softwarekomponenten: 36 % der Images enthalten Softwarekomponenten, für die Microsoft den Ausschluss aus IoT-Geräten empfiehlt, z. B. Paketerfassungstools (tcpdump, libpcap), die als Teil einer Angriffskette zur Netzwerkaufklärung verwendet werden können.

Firmware-Angriffe in Aktion

Viasat: Nutzen einer Firmware-Schwachstelle für Angriffe auf Satellitenkommunikation

Im Februar 2022 kappte ein Vorfall mit einem Satellitennetzwerk die Verbindung zu einem Kommunikationsnetzwerk. Dies hatte spürbare Auswirkungen auf ganz Europa. Das KA-SAT-System von Viasat erhielt eine große Menge an Datenverkehr, der die Verbindung vieler Modems trennte, und gegen das Netzwerk wurde ein Denial-of-Service-Angriff gestartet. Durch die Störung des Festnetzbreitbandnetzes war der betreiberseitige Remote-Zugriff auf Tausende von Windturbinen gestört, und auf den betroffenen Modems wurde bösartige Wiper-Schadsoftware eingeschleust. Die Störung betraf mehr als 30.000 Satellitenterminals, die von Unternehmen und Organisationen für die Kommunikation verwendet wurden.

Cyclops Blink: Ausnutzung einer Firmwarelieferkette für einen Angriff auf Firewall-Gateways

Für Akteure stellt die Entwicklung und der Ausbau einer C2- (Command and Control) und Angriffsinfrastruktur einen entscheidenden Erfolgsfaktor dar. Weil die Notwendigkeit einer stabilen C2-Infrastruktur größer geworden ist, haben sich Router aufgrund ihrer unregelmäßigen Patches und dem Fehlen umfassender Sicherheitslösungen zu einem beliebten Angriffsvektor entwickelt.

Microsoft geht bei der Technologie zur Analyse von Firmware Partnerschaften mit staatlichen Einrichtungen und der Industrie ein, um tiefere Einblicke in die Gerätesicherheit zu erhalten und sowohl für Hersteller als auch für Betreiber Sicherheit über den gesamten Lebenszyklus bereitzustellen.

Seit Juni 2019 verwendet eine mit einem Nationalstaat verbundene ATP-Gruppe (Advanced Persistent Threat) die modulare Schadsoftware Cyclops Blink für Angriffe auf anfällige WatchGuard-Firewallgeräte und ASUS-Router. Dabei wurden auf den Geräten Updates mit bösartiger Schadsoftware ausgeführt und sie anschließend für ein großes Botnet rekrutiert. Für eine erfolgreiche Infizierung der Geräte nutzt die Schadsoftware eine bekannte Schwachstelle aus, die Rechteeskalationen ermöglicht und die Akteure dadurch zur Verwaltung des jeweiligen Geräts befähigt. Einmal infiziert, lässt die Schadsoftware die Installation weiterer Module zu und verhindert Firmware-Updates. Es wurden kompromittierte Geräte beobachtet, die sich mit C2-Servern auf anderen WatchGuard-Geräten verbinden. Durch das Ausstellen vieler SSL-Zertifikate für ihre C2 auf verschiedenen TCP-Ports gewannen die Betreiber von Cyclops Blink privilegierten Remote-Zugriff auf Netzwerke. Dazu führten sie bösartige Firmware-Updates durch und umgingen herkömmliche Sicherheitsverfahren wie Scannen.

Wie Microsoft die Sicherheit der Lieferkette verbessert

Bei der Bewältigung dieser Herausforderungen im Zusammenhang mit der Sicherheit von IoT- und OT-Geräten arbeitet Microsoft mit staatlichen Einrichtungen und der Industrie zusammen (siehe die Erörterung auf Seite 66). Unser Beitrag besteht unter anderem im Einsatz von Technologie zur Analyse von Firmware, um den Betreibern Einblicke in den Sicherheitsstatus der Geräte in ihrem Netzwerk zu liefern. Auf diese Weise können die Kund*innen Geräte identifizieren und priorisieren, die zusätzlichen Schutz oder Upgrades benötigen oder ausgetauscht werden müssen. So erhöhen sie außerdem den Druck auf die Gerätehersteller, in die Gerätesicherheit zu investieren. Gleichzeitig unterstützen wir auch die Hersteller mit umfassenden Lösungen für die Entwicklung sicherer Geräte und die Einführung sicherer Entwicklungszyklen.

Eine weitere wichtige Komponente besteht darin, Hersteller und Betreiber mit einer robusten Infrastruktur zu versorgen, die ein Firmwareupdate ermöglicht, sobald Sicherheitsprobleme entdeckt und behoben wurden. Microsoft vereint die Firmwareanalyse und Defender for IoT mit Device Update for IoT Hub, um eine Lösung bereitzustellen, die den vollständigen Lebenszyklus der Sicherheit von IoT- und OT-Geräten umfasst. Dies sind wichtige Schritte bei der Realisierung unserer Vision, dass Kund*innen die Infrastruktur absichern, indem sie Geräte einführen, die einen Zero Trust-Ansatz für ihre IoT- und OT-Lösungen unterstützen.[18]

Angreifer attackieren zunehmend Schwachstellen in der Firmware von IoT-Geräten, um Unternehmensnetzwerke zu infiltrieren.

Umsetzbare Insights

1. Erhalten Sie detailliertere Einblicke in IoT-/OT-Geräte in Ihrem Netzwerk, und priorisieren Sie diese im Falle einer Kompromittierung nach Risiko für das Unternehmen.
2. Verwenden Sie Tools zum Scannen von Firmware, um potenzielle Sicherheitsschwächen zu verstehen, und kooperieren Sie mit den Anbietern, um zu bestimmen, wie Sie die Risiken für hochgefährdete Geräte abmildern können.
3. Stärken Sie die Sicherheit von IoT-/OT-Geräten, indem Sie von Ihren Anbietern die Umsetzung von Best Practices für einen sicheren Entwicklungslebenszyklus verlangen.

Links zu weiteren Informationen

- Assessment of the Critical Supply Chains Supporting the US Information and Communications Technology Industry

Auf Aufklärung basierende OT-Angriffe

Komplexe Lieferketten verwenden spezifische Designinformationen für die Planung des eigentlichen Systems. Von den unzähligen Ressourcen, aus denen sich diese Designinformationen zusammensetzen, ist die Projektdatei die sensibelste. Sie definiert die Umgebung und ihre Ressourcen. Diese Datei ist ein entscheidendes strategisches Ziel für Akteure, die es auf Zugriff abgesehen haben und einen erfolgreichen Angriff durchführen möchten, der vollständig auf die Umgebung zugeschnitten ist.

Angriffe auf industrielle Systeme zur Störung operativer Prozesse umfassen zwei Schritte.

1. Erstens muss der Angreifer auf das OT-Netzwerk zugreifen. Dies kann durch ein Eindringen über IoT-Geräte auf der Unternehmensseite des Netzwerks (Ebene 4 des Purdue-Modells) und das Überqueren der IT-OT-Grenze erfolgen. Diese Grenze wird herkömmlicherweise durch Firewalls und Netzwerkgeräte gezogen, die die Umgebung in Betriebs- und Steuerungsebenen unterteilen.
2. Zweitens müssen die Netzwerkgeräte identifiziert werden. Industrielle Systeme verwenden Standard-geräte und -komponenten in stark angepassten Archi-tekturen, die speziell für ihre Umgebungen entwickelt wurden. Eines dieser Standardgeräte ist die speicher-programmierbare Steuerung (SPS). Jeder Hersteller entwickelt einzigartige Schnittstellen und Funktionen für seine SPSs, die eine entscheidende Komponen-te industrieller Systeme bilden. Über angepasste Schemata, die speziell auf die Umgebungen der Kund*innen ausgelegt sind, werden diese Geräte weiter konfiguriert.

In der Projektdatei wird die individuelle Konfiguration jeder einzelnen SPS beschrieben. Sie enthält auch die Definition der Umgebung und ihrer Ressourcen, den Kontaktplan und vieles mehr.

In den meisten Umgebungen, in denen Nachweise für einen Angriff vorliegen, zeigt die Analyse eine Zeitachse, die bereits vor dem Angriff beginnt und weit über die Länge des eigentlichen Angriffs hinausgeht. Akteure investieren oft Monate in die Remote-Simulation der Umgebung und ihrer Ressourcen und unternehmen dabei viele Versuche, ein Modell zu konstruieren und ihren gezielten Angriff vorzubereiten. Da sich Umgebungen laufend verändern und neue Geräte integriert werden, entstehen Schwachstellen vor allem bei den Daten in den Projekt- und Konfigurationsdateien. Der Diebstahl einer Projektdatei kann einen Angriff um Wochen oder Monate beschleunigen und Angreifer in die Lage versetzen, die Zielumgebung schnell und präzise zu modellieren. Dies erschwert das Erkennen bösartiger Aktivitäten.

Industroyer und Incontroller

Wir haben verstärkt Angriffe auf Organisationen, kritische Infrastruktur und Regierungsziele durch staatlich geförderte Akteure beobachtet, die modulare Schadsoftware und Angriffsframeworks verwenden. Neue Versuche, kritische Prozesse in der Ukraine zu stören, unterstreichen die zunehmende Bedrohung durch aufklärungsbasierte OT-Angriffe, die in hohem Maße auf ihre Zielumgebungen zugeschnitten sind. Die erweiterten Aufklärungs- und Forschungsphasen, die von nationalstaatlichen Cyberakteuren durchgeführt werden, deuten auf eine Strategie hin, bei der Mittel der Cyberkriegsführung remote für das Ausschalten von Infrastruktur eingesetzt werden, um bestimmte strategische oder operative Ziele in einem gemischten Ansatz aus cyberkinetischen Operationen und politischer Strategie zu erreichen.

Wir haben eine wachsende Bedrohung durch auf Aufklärung basierende OT-Angriffe beobachtet, die in hohem Maße auf ihre Zielumgebungen zugeschnitten sind.

Auf Aufklärung basierende OT-Angriffe

Fortsetzung

Anfang 2022 wurden zwei anpassbare kritische OT-Angriffe identifiziert. Ein cyberphysischer Angriff auf elektrische Umspannwerke und Schutzrelais in der Ukraine wurde mit angepasster Schadsoftware durchgeführt. Dazu gehörte auch eine Variante von Industroyer, einer Schadsoftware, von der bekannt ist, dass sie nach ihrem Aufkommen 2016 Stromausfälle in der Ukraine verursacht hat.

Industroyer2 ist die erste bekannte erneute Bereitstellung von bösartiger OT-Angriffsschadsoftware gegen ein neues Ziel. Sie nutzte ein Plug-in für das IEC104-Protokoll (Standardprotokoll für die Überwachung und Steuerung von Stromsystemen), das für Industroyer entwickelt wurde, und war überwiegend auf SPS-ähnliche Remote-Terminalgeräte mit der Modellnummer ABB RTU540/560 ausgerichtet. Der Urheber dieser Schadsoftware nutzte Wissen über die Umgebung des Opfers, um wiederholt Befehle an vordefinierte Outputs auszugeben, mit denen sichergestellt wurde, dass sie nicht manuell aktiviert werden konnten. Dies sorgte für längere Stromausfälle und verschärfte die schädlichen Auswirkungen.

Incontroller, ein modulares Angriffsframework, das im selben Zeitraum identifiziert wurde, ist ein modulares Toolkit, das die Vorlaufzeit für das Eindringen in und Angreifen von OT-Geräten reduziert, indem es ältere Sicherheitslösungen umgeht. Das universelle Toolkit verfügt über Datenerfassungs-, Aufklärungs- und Angriffsfunktionen, die hochgradig an unterschiedliche Umgebungen anpassbar sind und sich erheblich auf die Ausforschungsphase für einen OT-Angriff auswirken. Dies reduziert die erforderliche Zeit für die Aufklärung und unterstützt die Simulation von Umgebungen, da es die Informationen über Geräte und ihre Konfigurationen extrahiert.

Das Incontroller-Framework unterstützt Protokolle für SPSs von Schneider Electric und Omron und sammelt Informationen wie Firmwareversion, Modelltyp und vernetzte Geräte. Das Toolkit kann Befehle ausgeben, die Konfigurationen ändern und Outputs ein- und ausschalten. Sobald auf eine Umgebung zugegriffen wird, unterstützt das Framework das Implantieren von Hintertüren in den Geräten, die das Einschleusen weiterer Nutzlasten, das Herstellen von Schwachstellen für mehr Zugriffspunkte, das Hochladen des Kontaktplans und die Fähigkeit zum Einleiten von DoS-Angriffen ermöglichen. Durch die generische Natur des Toolkits können Akteure eine Umgebung schnell angreifen, ohne für jede SPS oder für jeden Standort neue Angriffe schreiben zu müssen. Auf diese Weise kann der Akteur problemlos über viele Branchen hinweg mit unterschiedlichen Arten von Maschinen interagieren.

Umsetzbare Insights

1. Vermeiden Sie die Übertragung von Dateien mit Systemdefinitionen über unsichere Kanäle oder an nicht relevante Mitarbeiter*innen.
2. Wenn die Übertragung solcher Dateien unvermeidlich ist, müssen Sie die Aktivitäten im Netzwerk überwachen und sicherstellen, dass die Ressourcen sicher sind.
3. Schützen Sie Entwicklungsstationen durch eine Überwachung mit EDR-Lösungen.
4. Reagieren Sie proaktiv auf Vorfälle in OT-Netzwerken.
5. Stellen Sie eine kontinuierliche Überwachung bereit, z. B. Defender for IoT.

Fußnoten

1. Siehe z. B. Revised Directive on Security of Network and Information Systems (NIS2) | Shaping Europe's digital future (europa.eu); https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2020:595:FIN&rid=1; Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 (homeaffairs.gov.au); Chile: Bill for cybersecurity and critical information infrastructure introduced in Senate | News post | DataGuidance; Japan passes economic security bill to guard sensitive technology | The Japan Times; Review of the Cybersecurity Act and Update to the Cybersecurity Code of Practice for CIIs (csa.gov.sg); Proposal for legislation to improve the UK's cyber resilience – GOV.UK (www.gov.uk); Telecommunications (Security) Act 2021 (legislation.gov.uk); Updating the NIST Cybersecurity Framework – Journey To CSF 2.0 | NIST
2. Cert-In – Startseite
3. Initiation of consultation on introduction of cyberattack reporting obligation (admin.ch)
4. Siehe z. B. Untitled (house.gov)
5. Cyber Resilience Act | Shaping Europe's digital future (europa.eu)
6. Siehe z. B. Microsoft Security Development Lifecycle
7. Siehe z. B. Generating Software Bills of Materials (SBOMs) with SPDX at Microsoft – Engineering@Microsoft; siehe außerdem z. B. The Minimum Elements For a Software Bill of Materials (SBOM) | National Telecommunications and Information Administration (ntia.gov)
8. Siehe z. B. https://www.microsoft.com/en-us/msrc/cvd
9. The Product Security and Telecommunications Infrastructure (PSTI) Bill – Product Security Factsheet – GOV.UK (www.gov.uk)
10. Commission strengthens cybersecurity of wireless devices and products (europa.eu)
11. Cloud Certification Scheme: Building Trusted Cloud Services Across Europe – ENISA (europa.eu)
12. Zertifizierung – ENISA (europa.eu)
13. https://github.com/microsoft/sbom-tool GitHub-Microsoft/SBOM-Tool: Das SBOM-Tool ist ein hochgradig skalierbares Tool der Enterpriseklasse zur Erstellung SPDX 2.2-kompatibler SBOMs für eine Vielzahl von Artefakten.
14. https://www.zdnet.com/article/ripple20-vulnerabilities-will-haunt-the-iot-landscape-for-years-to-come
15. IoT/OT Innovation Critical but Comes with Significant Risks (Dec 2021): https://www.microsoft.com/security/blog/2021/12/08/new-research-shows-iot-and-ot-innovation-is-critical-to-business-but-comes-with-significant-risks/
16. Uncovering Trickbot's use of IoT devices in C2 Infrastructure (März 2022): https://www.microsoft.com/security/blog/2022/03/16/uncovering-trickbots-use-of-iot-devices-in-command-and-control-infrastructure/
17. Die IoT Show auf Channel 9, Episode über das Scannen von IoT-Firmware (Mai 2022): https://docs.microsoft.com/en-us/shows/internet-of-things-show/iot-device-firmware-security-scanning-with-azure-defender-for-iot
18. How to apply a Zero Trust approach to your IoT solutions (Mai 2021): https://www.microsoft.com/security/blog/2021/05/05/how-to-apply-a-zero-trust-approach-to-your-iot-solutions/

Einflussnahme im Cyberspace

Die heutigen ausländischen Operationen zur Einflussnahme nutzen neue Methoden und Technologien. Das macht ihre Kampagnen, die auf die Zersetzung von Vertrauen abzielen, noch effizienter und effektiver.

Übersicht über

Operationen zur Einflussnahme im Cyberspace

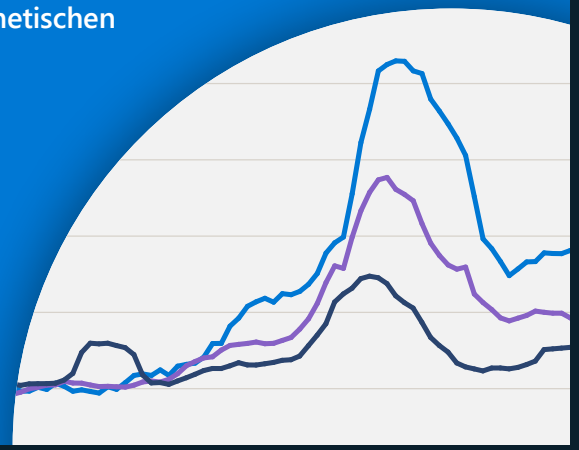
Die heutigen ausländischen Operationen zur Einflussnahme nutzen neue Methoden und Technologien. Das macht ihre Kampagnen, die auf die Zersetzung von Vertrauen abzielen, noch effizienter und effektiver.

Nationalstaaten nutzen zunehmend ausgeklügelte Operationen zur Einflussnahme, um Propaganda zu streuen und die öffentliche Meinung sowohl im Inland als auch international zu beeinflussen. Diese Kampagnen untergraben Vertrauen, erhöhen die Polarisierung und bedrohen demokratische Prozesse. Erfahrene Akteure, die sich als Advanced Persistent Manipulators betätigen, nutzen traditionelle Medien zusammen mit dem Internet und Social Media, um den Umfang, die Größenordnung und die Effizienz ihrer Kampagnen und deren außerordentliche Auswirkungen auf die weltweiten Informationsnetzwerke enorm zu steigern.
Im vergangenen Jahr wurden wir Zeugen, wie solche Operationen als Teil der russischen hybriden Kriegsführung in der Ukraine eingesetzt wurden. Wir erlebten aber auch, wie Russland und andere Nationen wie China und Iran in zunehmendem Maße von Social Media gestützte Propagandaaktionen durchführen, um ihren weltweiten Einfluss auszubauen.

Operationen zur Einflussnahme im Cyberspace werden immer raffinierter, weil immer mehr Regierungen und Nationalstaaten sie nutzen, um Meinungen zu beeinflussen, Gegner zu diskreditieren und Zwietracht zu säen.

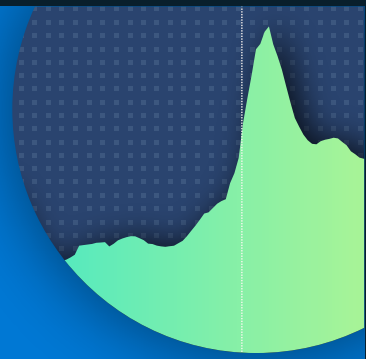
Weitere Informationen finden Sie auf S. 74

Um maximalen Effekt zu erzielen, umfasste der russische Angriffskrieg gegen die Ukraine auch Operationen zur Beeinflussung des Cyberspace, gepaart mit eher herkömmlichen Cyberangriffen und kinetischen Militäroperationen.



Weitere Informationen finden Sie auf S. 76

Während der gesamten COVID-19-Pandemie haben Russland, Iran und China Propaganda- und Einflusskampagnen häufig als strategisches Instrument zur Erreichung von breiter gefassten politischen Zielen eingesetzt.



Weitere Informationen finden Sie auf S. 76

Bei synthetischen Medien sind hohe Zuwächse zu verzeichnen. Dies liegt an der Verbreitung von Tools, die das Erstellen und Verbreiten extrem realistischer künstlicher Bild-, Video- und Tonaufnahmen sehr einfach machen. Technologie für digitale Provenienz, die die Quelle von Medienressourcen bescheinigt, verspricht, den Missbrauch zu bekämpfen.

Weitere Informationen finden Sie auf S. 80

Ein ganzheitlicher Ansatz zum Schutz vor Operationen zur Einflussnahme im Cyberspace

Microsoft baut bei der Bekämpfung von Operationen zur Einflussnahme im Cyberspace auf der bereits ausgereiften Cyber Threat Intelligence-Infrastruktur auf. Unsere Strategie besteht darin, Propagandakampagnen von ausländischen Aggressoren zu entdecken, zu unterbinden, abzuwehren und abzuschrecken.

Weitere Informationen finden Sie auf S. 83

Einführung

Demokratie braucht vertrauenswürdige Informationen, um gedeihen zu können. Ein zentraler Schwerpunkt für Microsoft liegt auf Operationen zur Einflussnahme im Cyberspace, die von Nationalstaaten entwickelt und fortwährend durchgeführt werden. Diese Kampagnen untergraben Vertrauen, erhöhen die Polarisierung und bedrohen demokratische Prozesse.

Beeinflussungsoperationen aus dem Ausland waren schon immer eine Bedrohung für die Informationsnetzwerke. Was jedoch im Zeitalter des Internets und der sozialen Medien anders ist, ist der weitaus größere Umfang, die Skalierbarkeit und Effizienz von Kampagnen sowie die überdimensionierten Auswirkungen, die sie auf die Integrität der weltweiten Informationsnetzwerke haben können.

Das alte Sprichwort, dass „eine Lüge es um die halbe Welt schafft, bevor die Wahrheit auch nur ihre Schuhe anziehen konnte“, bewahrheitet sich nun mit Daten. Eine Studie des Massachusetts Institute of Technology (MIT)[1] ergab, dass Unwahrheiten mit einer um 70 % höheren Wahrscheinlichkeit weiterverbreitet werden als die Wahrheit und sie die ersten 1.500 Personen sechsmal schneller erreichen. Es wird immer schwieriger, die komplexen Informationsnetzwerke zu durchschauen, weil Propagandakampagnen im Internet und in sozialen Netzwerken florieren und das Vertrauen in traditionelle Nachrichten untergraben. In einer Studie aus dem Jahr 2021[2] gaben nur 7 % der Erwachsenen in den USA an, dass sie „sehr viel“ Vertrauen in Zeitungen, das Fernsehen und Radionachrichten haben, wohingegen 34 % vermeldeten, „überhaupt kein“ Vertrauen zu haben.

Microsoft hat daran gearbeitet, die wichtigsten Akteure, Bedrohungen und Taktiken im ausländischen Einflussbereich des Cyberspace zu identifizieren und die gewonnenen Erkenntnisse weiterzugeben. Im Juni dieses Jahres haben wir einen umfassenden Bericht über die aus der Ukraine gewonnenen Erkenntnisse veröffentlicht. Darin enthalten war eine genaue Betrachtung der russischen Operationen zur Einflussnahme im Cyberspace.[3]

Wir untersuchen auch, wie moderne Technologien z. B. bei Deepfakes als Waffen genutzt werden und die Glaubwürdigkeit von Journalisten untergraben können. Wir arbeiten mit der Industrie, staatlichen Einrichtungen und der akademischen Welt zusammen, um bessere Wege zum Erkennen synthetischer Medien und zum Wiederherstellen von Vertrauen zu entwickeln – beispielsweise durch Systeme mit künstlicher Intelligenz (KI), die Fälschungen erkennen können.

Die sich schnell wandelnde Natur von Informationsnetzwerken und Onlinepropaganda von Nationalstaaten, einschließlich der Verschmelzung traditioneller Cyberangriffe mit Beeinflussungsoperationen und der Einmischung in demokratische Wahlen, erfordert einen gesamtgesellschaftlichen Ansatz, um sowohl Online- als auch Offlinebedrohungen für die Demokratie entgegenzuwirken.

Microsoft setzt sich für die Unterstützung einer gesunden Informationsinfrastruktur ein, in der vertrauenswürdige Nachrichten und Informationen gedeihen. Wir entwickeln Tools und Funktionen zur Erkennung von Bedrohungen, um die sich wandelnden und wachsenden Risiken durch nationalstaatliche Beeinflussungsoperationen bekämpfen. Um diese Arbeit zu ermöglichen, haben wir vor kurzem Miburo Solutions erworben, arbeiten mit unabhängigen Validierern wie dem Global Disinformation Index und NewsGuard zusammen und beteiligen uns, teils in führender Rolle, an Partnerschaften mit mehreren Interessengruppen, darunter die Coalition für Content Provenance and Authenticity (C2PA). Nur wenn wir zusammenarbeiten, können wir es erfolgreich mit jenen aufnehmen, die unsere demokratischen Prozesse und Institutionen untergraben wollen.

Teresa Hutson

Vice President, Technology and Corporate Responsibility

Trends bei Operationen zur Einflussnahme im Cyberspace

Operationen zur Einflussnahme im Cyberspace werden durch die schnelle technologische Entwicklung immer ausgefeilter. Wir erleben eine Überlagerung und Erweiterung der Tools, die im Rahmen von herkömmlichen Cyberangriffen eingesetzt werden und jetzt bei Operationen zur Einflussnahme im Cyberspace zur Anwendung kommen. Darüber hinaus beobachten wir mehr Koordination und Verstärkung zwischen Nationalstaaten.

Mit der Übernahme von Miburo Solutions, einem Unternehmen, das sich auf die Analyse ausländischer Beeinflussungsoperationen spezialisiert hat, hat Microsoft in diesem Jahr in die Bekämpfung ausländischer Beeinflussungsoperationen investiert. Durch das Zusammenbringen dieser Analyst*innen mit den Bedrohungskontextanalyst*innen von Microsoft entstand das Digital Threat Analysis Center (DTAC). Das DTAC analysiert nationalstaatliche Bedrohungen und erstattet über sie Bericht, darunter sowohl Cyberangriffe als auch Beeinflussungsoperationen, bündelt Informationen und Threat Intelligence mit geopolitischer Analyse, um Insights bereitzustellen, und liefert die Grundlagen für effektive Reaktionen und Schutzmaßnahmen.

Mehr als drei Viertel der Menschen auf der ganzen Welt gaben an, dass sie sich um die Nutzung von Informationen als Waffe Sorgen machen,[4] und unsere Daten stützen diese Bedenken. Microsoft und seine Partner haben verfolgt, wie nationalstaatliche Akteure Beeinflussungsoperationen nutzen, um ihre strategischen und politischen Ziele zu erreichen. Neben destruktiven Cyberangriffen und Initiativen zur Cyberspionage nutzen autoritäre Regime zunehmend Operationen zur Einflussnahme im Cyberspace, um Meinungen zu beeinflussen, Gegner zu diskreditieren, Angst zu schüren und die Realität zu verzerren.

Diese ausländischen Operationen zur Einflussnahme im Cyberspace verlaufen in der Regel in drei Phasen:

Prä-Positionierung

Genau wie bei der Bereitstellung von Schadsoftware im Computernetzwerk in einer Organisation werden bei Operationen zur Einflussnahme im Cyberspace falsche Narrative vorbereitend in der öffentlichen Domäne des Internet platziert. Diese Taktik der Prä-Positionierung war bei herkömmlichen Cyberaktivitäten lange hilfreich, insbesondere, wenn IT-Administratoren nur die jüngsten Aktivitäten in ihrem Netzwerk scannen. Schadsoftware, die längere Zeit in einem Netzwerk schlummert, kann später noch effektiver eingesetzt werden. Falsche Narrative, die unbemerkt im Internet stehen, können spätere Verweise auf sie glaubwürdiger erscheinen lassen.

Einführung

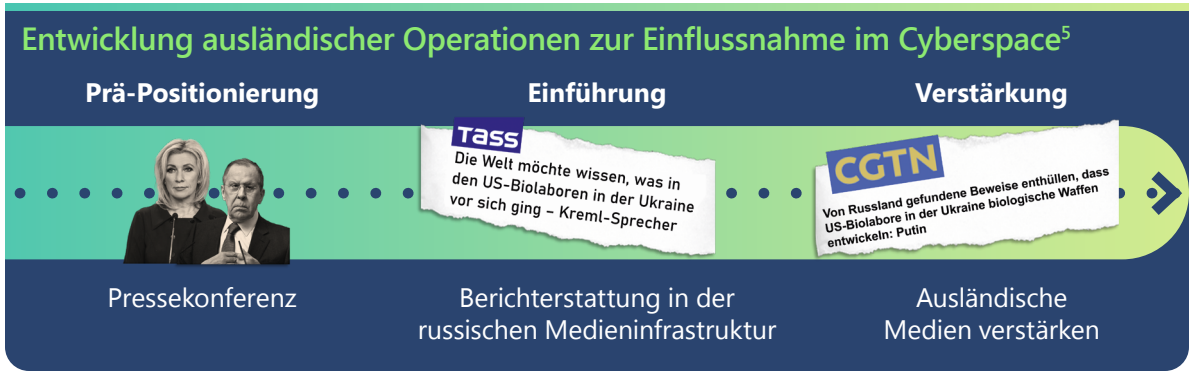
Häufig wird dann, wenn es zum Erreichen der Ziele eines Akteurs am günstigsten erscheint, eine koordinierte Kampagne gestartet, um die Narrative über staatlich gestützte und beeinflusste Medien und Social Media-Kanäle zu verbreiten.

Verstärkung

Schließlich verstärken die staatlich kontrollierten Medien und Sprachrohre die Narrative innerhalb der jeweiligen Zielgruppen. Oft wird die Reichweite der Narrative durch technische Wegbereiter unwissentlich noch vergrößert. Beispielsweise kann Onlinewerbung bei der Finanzierung der Aktivitäten helfen, und Systeme zur koordinierten Content-Verbreitung können Suchmaschinen fluten.

Dieser dreistufige Ansatz kam beispielsweise Ende 2021 zum Einsatz, um das falsche russische Narrativ von angeblichen Biowaffen und Biolaboren in der Ukraine zu stützen. Dieses Narrativ wurde erstmalig am 29. November 2021 auf YouTube hochgeladen. Dies geschah im Rahmen einer regelmäßigen englischsprachigen Sendung von einem amerikanischen Auswanderer, der jetzt in Moskau lebt und behauptete, dass von den USA finanzierte Biolabore in der Ukraine mit Biowaffen in Zusammenhang stünden. Die Geschichte blieb monatelang weitgehend unbemerkt. Als am 24. Februar 2022 russische Panzer die Grenze überquerten, wurde das Narrativ in die Schlacht geschickt. Ein Datenanalyseteam bei Microsoft identifizierte zehn von der russischen Seite kontrollierte oder beeinflusste Nachrichtenseiten, die am 24. Februar gleichzeitig Berichte veröffentlichten, die auf die „Meldung aus dem letzten Jahr" verwiesen, um sich Glaubwürdigkeit zu verleihen. Darüber hinaus gaben Vertreter des russischen Außenministeriums Pressekonferenzen, in denen sie die Saat der Falschbehauptungen über US-Biolabore weiter in der Informationslandschaft verstreuten. Anschließend machten sich von Russland finanzierte Teams daran, dass Narrativ auf Social Media und auf Internetseiten weiter zu verbreiten und zu verstärken.

Wir erleben, wie autoritäre Regime auf der ganzen Welt zusammenarbeiten, um Informationsnetzwerke zu ihrem eigenen Vorteil zu unterminieren. So haben Russland, der Iran und China beispielsweise während der gesamten COVID-19-Pandemie Propaganda und Beeinflussungsoperationen mit einer Mischung aus offenen, teilweise verdeckten und ganz verdeckten Verbreitungsmethoden eingesetzt, um Demokratien anzugreifen und ihre geopolitischen Ziele voranzutreiben (siehe weitere Erörterung auf Seite 76). Die drei Regime bespielten gegenseitig ihre Nachrichten- und Informationsnetzwerke, um die bevorzugten Narrative zu befeuern. Ein Großteil der Meldungen bestand aus Kritik oder Verschwörungstheorien über die USA und ihre Verbündeten, mit denen Regierungsvertreter*innen in offiziellen Stellungnahmen hausieren gingen und dabei gleichzeitig ihre eigenen Impfstoffe und Maßnahmen in Bezug auf COVID-19 als denen der USA und anderer Demokratien überlegen anpriesen. Indem sie sich gegenseitig verstärkten, schufen die staatlich betriebenen Nachrichtenmedien eine Infrastruktur, in der negative Berichterstattung über Demokratien – oder positive Berichterstattung über Russland, den Iran und China –, die von einer Anstalt produziert worden war, von anderen verstärkt wurde.



Illustration, wie sich Narrative über US-Biolabore und biologische Waffen über die drei allgemeinen Phasen in vielen ausländischen Beeinflussungsoperationen verbreiten. Die Phasen sind: Prä-Positionierung, Einführung und Verstärkung.

Trends bei Operationen zur Einflussnahme im Cyberspace

Fortsetzung

Um die Herausforderung noch größer zu machen, könnten Technologieentitäten aus dem privaten Sektor diese Kampagnen unwissentlich noch unterstützen. Wegbereiter können Unternehmen sein, die Internetdomänen registrieren, Webseiten hosten, Material auf Social Media und Suchseiten bewerben, Datenverkehr kanalisieren und über digitale Werbung dabei helfen, für diese Betätigungen zu bezahlen. Organisationen müssen sich der Tools und Methoden bewusst sein, die von autoritären Regimen für Operationen zur Einflussnahme im Cyberspace eingesetzt werden, damit sie diese Kampagnen und ihre Verbreitung eindämmen können. Es gibt auch einen wachsenden Bedarf daran, Verbraucher*innen dabei zu helfen, zuverlässige Methoden zum Erkennen von ausländischen Beeinflussungsmethoden und zum Begrenzen der Verbreitung der entsprechenden Narrative oder Inhalte zu entwickeln.

Operationen zur Einflussnahme im Cyberspace, einschließlich autoritärer Propaganda, sind eine Bedrohung für Demokratien auf der ganzen Welt, weil sie Vertrauen untergraben, die Polarisierung verstärken und demokratische Prozesse bedrohen.

Um die Transparenz zu erhöhen und solche Beeinflussungskampagnen offenzulegen und zu stoppen, bedarf es einer verstärkten Koordination sowie eines besseren Informationsaustauschs zwischen staatlichen Stellen, dem Privatsektor und der Zivilgesellschaft.

Weltweit sorgen sich mehr als drei Viertel der Menschen darum, wie Informationen als Waffen genutzt werden.

Operationen zur Einflussnahme während der COVID-19-Pandemie und Russlands Angriffskrieg gegen die Ukraine

Nationalstaaten, die die Informationsumgebung während der Pandemie und auch beim russischen Angriffskrieg gegen die Ukraine kontrollieren möchten, liefern starke Beispiele dafür, wie autoritäre Regime Cyber- und Informationsprozesse verschmelzen.

COVID-19-Propaganda

Russland, der Iran und China haben während der gesamten COVID-19-Pandemie Propaganda und Beeinflussungskampagnen eingesetzt. COVID-19 nahm bei diesen Kampagnen eine zentrale Stellung ein, und zwar auf zweierlei Weise:

1. Darstellungen der Pandemie selbst.
2. Kampagnen, die COVID-19 als strategisches Instrument zur Erreichung breiterer politischer Ziele nutzten.

Das breiter gefasste Ziel dieser Kampagnen hat zwei Dimensionen: erstens das Untergraben von Demokratien, demokratischen Institutionen und des Images der USA und ihrer Verbündeten auf der Weltbühne, und zweitens das Stärken der eigenen Position sowohl im Inland als auch international.

Ein Beispiel dafür ist der starke Kontrast zwischen Botschaften von bekannten russischen Accounts und Medienorganisationen an englischsprachige Leser*innen in Bezug auf die Impfstoffe und den Ernst von COVID-19 und der diesbezüglichen Kommunikation der russischen Regierung mit dem eigenen Volk.

Die häufigsten Themen in den zehn am häufigsten angesehenen Coronavirus-Meldungen auf RT.com
(Oktober 2021 – April 2022)

Propaganda gegen Impfstoffe zielte auf nicht russische Leser ab

Russisch (Übersetzung)	Deutsch
„Lockdowns und Booster verhindern eine Übertragung“	„Impfungen können die Übertragung nicht einschränken und sind gegen neue Stämme wirkungslos“
„Russische Prominente werden positiv getestet“	„Der Pfizer-Impfstoff hat gefährliche Nebenwirkungen“
„Fallzahlen und Todesfälle steigen in Russland an“	„Massenimpfung ist politisch motiviert“
„Der Sputnik V-Impfstoff ist hoch wirksam“	„Pfizer und Moderna führen unregulierte Studien durch“
„Impfnachweis in öffentlichen Verkehrsmitteln erforderlich“	

Russisches Messaging zu COVID-19 unterscheidet sich je nach Sprache.

Kampagnen, die den Ursprung des COVID-19-Virus verschleiern wollten, sind ein weiteres Beispiel. Seit dem Ausbruch der Pandemie hat russische, iranische und chinesische COVID-19-Propaganda die Berichterstattung der jeweils anderen unterstützt, um diese zentralen Themen zu verstärken. Ein Großteil dieser Berichterstattung bestand aus Kritik an oder Verschwörungstheorien über die USA. Indem sie sich regelmäßig gegenseitig verstärkten, schufen die staatlich betriebenen Nachrichtenmedien eine Infrastruktur, in der negative Berichterstattung über Demokratien – oder positive Berichterstattung über Russland, den Iran und China –, die von einer Anstalt produziert worden war, von anderen erneut aufgegriffen und praktisch multipliziert wurde.

Ein solches Beispiel ist die frühzeitige Andeutung russischer und iranischer Staatsmedien, dass COVID-19 eine von den USA geschaffene Biowaffe sein könnte. Diese Behauptung zirkulierte zu Beginn der Pandemie auf randständigen Verschwörungswebseiten, nachdem ein Juraprofessor in einem Interview behauptet hatte, dass COVID-19 seiner Meinung nach als Waffe erschaffen worden sei.[6] Nach der Veröffentlichung des Interviews auf einigen Websites mit beschränkter Reichweite griffen staatliche Medien die Geschichte auf. PressTV, ein iranisches englisch- und französischsprachiges Medienunternehmen, das von der iranischen Regierung finanziert wird[7], veröffentlichte im Februar 2020 eine Story auf Englisch mit dem Titel „Is Coronavirus a US Biowarfare Weapon as Francis Boyle Believes?“ (Ist das Coronavirus eine US-Biowaffe, wie Francis Boyle glaubt?) Der Artikel suggerierte, dass die Vereinigten Staaten hinter dem COVID-19-Ausbruch steckten. Wörtlich hieß es: „In allen Kriegen der USA kamen radiologische, biologische und andere geächtete Waffen zum Einsatz und forderten in den betroffenen Gebieten verheerende Opferzahlen unter der Bevölkerung.“[8] Diese Meinung wurde in russischen Staatsmedien und Konten der chinesischen Regierung widergespiegelt. Russia Today (RT) – ein staatlicher Nachrichtensender, der für seine Rolle bei der Verbreitung von Propaganda des Kremls bekannt ist,[9] – veröffentlichte mindestens eine Story, die Aussagen von iranischen Offiziellen stützte, denen zufolge COVID-19 ein „Produkt eines US-Bioangriffs gegen den Iran und China“ sei,[10] und veröffentlichte Posts in Social Media, die dasselbe besagten. Am 27. Februar 2020 veröffentlichte RT beispielsweise folgenden Tweet: Bitte Handzeichen: Wer wäre nicht überrascht, wenn herauskäme, dass das #coronavirus eine Biowaffe ist?“[11]

Der Krieg in der Ukraine – Propaganda als Kriegswaffe

Russlands Angriffskrieg gegen die Ukraine liefert ein deutliches Beispiel dafür, wie Operationen zur Einflussnahme im Cyberspace mit eher traditionellen Cyberangriffen und Militäroperationen auf dem Boden kombiniert werden können, um maximale Wirkung zu erzielen.

Im Vorfeld des Angriffs beobachteten Threat Intelligence-Analysten von Microsoft, wie mindestens sechs verschiedene russische Akteure mehr als 237 Cyberangriffe gegen die Ukraine starteten. Diese Kampagnen versuchten, Dienste und Institutionen zu schwächen, den ukrainischen Zugriff auf verlässliche Informationen zu stören und Zweifel über die Führung des Landes zu säen.

Operationen zur Einflussnahme während der COVID-19-Pandemie und Russlands Angriffskrieg gegen die Ukraine

Fortsetzung

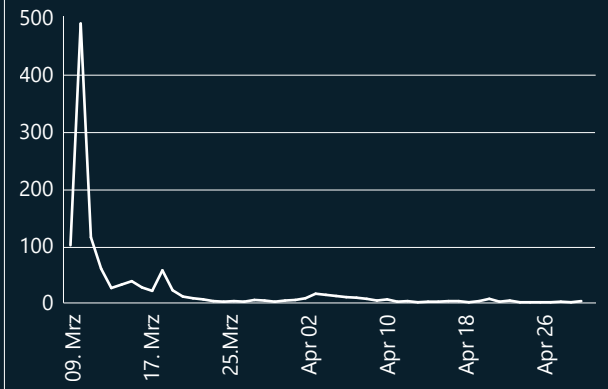
In einem Microsoft-Bericht aus April 2022 haben wir gezeigt, wie Russland in einem offensichtlichen Versuch, die Informationsumgebung in Kiew zu kontrollieren, einen Raketenangriff gegen einen Fernsehturm durchführte und am gleichen Tag ein großes ukrainisches Medienunternehmen mit destruktiver Schadsoftware angriff.[12]

In einem weiteren Beispiel für das Zusammenwirken von Cyberangriffen und Beeinflussungsoperationen wurden von russischer Seite E-Mails an ukrainische Bürger*innen gesendet, die vorgaben, von Bewohner*innen Mariupols zu stammen. Darin wurde der ukrainischen Regierung vorgeworfen, für die Eskalation des Krieges verantwortlich zu sein, und die vermeintlichen Landsleute wurden zum Widerstand gegen ihre Regierung aufgerufen. Diese E-Mails waren gezielt (mit Namen) an die jeweiligen Empfänger der E-Mail adressiert. Das liegt nahe, dass deren Daten möglicherweise in einem früheren Cyberangriff, der auf Spionage abzielte, gestohlen worden waren. Die E-Mails enthielten keine bösartigen Links, was darauf hindeutet, dass die Absicht in einer reinen Beeinflussungsoperation lag.

Angeblich gehacktes, durchgesickertes oder anderweitig sensibles Material ist eine gängige Taktik, die von russischen Akteuren bei Beeinflussungsoperationen eingesetzt wird. Während des Krieges in der Ukraine haben prorussische Social Media-Kanäle Inhalte verbreitet, die sie als durchgesickertes oder sensibles Material von ukrainischen Quellen ausgaben. Durchgesickertes oder sensibles Material wird von russischen Sendern oder Nachrichtenunternehmen als Teil einer breiter gefassten Beeinflussungsstrategie verwendet, um das Vertrauen in Institutionen zu zersetzen und Zweifel über Mainstream-Narrative zu streuen. Diese Informationen können manipuliert sein, um Propaganda gegen die Ukraine und den Westen zu entwickeln, das Vertrauen in die digitale Sicherheit zu schwächen und westliche Unterstützungsmaßnahmen für die Ukraine auszuhöhlen.

Russland nutzte noch weitere Informationsangriffe, um die öffentliche Meinung nach den Ereignissen vor Ort zu gestalten, um Fakten zu verschleiern oder zu untergraben. Am 7. März hat Russland beispielsweise über eine Eingabe bei den Vereinten Nationen (UN) ein Narrativ lanciert, dass eine Geburtsklinik in Mariupol, Ukraine, evakuiert worden sei und als militärische Einrichtung genutzt werde. Am 9. März bombardierte Russland das Krankenhaus. Nach der Nachricht von der Bombardierung setzte Russlands UN-Repräsentant, Dmitry Polyanskiy, einen Tweet ab, dass es sich bei der Bombardierung um „Fake News" handele, und zitierte Russlands frühere Behauptungen über die angebliche militärische Nutzung. In den zwei Wochen nach dem Angriff auf das Krankenhaus forcierte Russland dieses Narrativ auf allen russisch kontrollierten Websites.

Domänen mit Datenverkehr
(9. März 2022 – 30. April 2022)



Für etwa zwei Wochen lang veröffentlichten Propagandawebsites Storys über die Geburtsklinik. Am 1. April 2022 lebte die Berichterstattung kurz wieder auf. Quelle: Microsoft AI for Good Lab.

Satellitenbilder einer Geburtsklinik in Mariupol im Februar und Mai 2022

Eine Microsoft-Analyse der Satellitenbilder ergab, dass die Geburtsklinik bombardiert wurde. Das erste Foto ist vom 24. Februar 2022 und das zweite vom 24. März 2022. Quelle des Fotos: Planet Labs.

Russlands Schönreden seiner Gräueltaten hat sich während des Krieges fortgesetzt. Ende Juni 2022 stellten russische Medien und Influencer die Bombardierung eines Einkaufszentrums beispielsweise als gerechtfertigt und notwendig dar und behaupteten fälschlicherweise, dass es nicht als Einkaufszentrum verwendet wurde, sondern als Waffenlager für die territorialen ukrainischen Verteidigungskräfte.[13] Mehrere prorussische Blogger posteten und verstärkten auf Telegram Inhalte, die das Narrativ einer „False Flag" beförderten. Dabei verweisen sie auf angebliche Anzeichen einer Fälschung, unter anderem die Anwesenheit von Menschen in Militäruniform auf Bildaufnahmen vom Ort des Geschehens[14] und die Abwesenheit von Frauen.[15] Russland startete Kampagnen, bei denen es sich auf ein ausgestaltetes System von Propaganda-Messengern und -Medien stützte. Diese Storys online zu verstärken, versetzte Russland in die Lage, die Schuldzuweisung auf die internationale Bühne abzulenken und sich aus der Verantwortung zu stehlen.

Nationalstaaten wie Russland verstehen den Wert von Informationen aus geschlossenen Quellen bei der Beeinflussung der öffentlichen Wahrnehmung. Dabei verbreiten sie die Gegennarrative mithilfe von „Hack-and-Leak"-Kampagnen und säen Misstrauen.

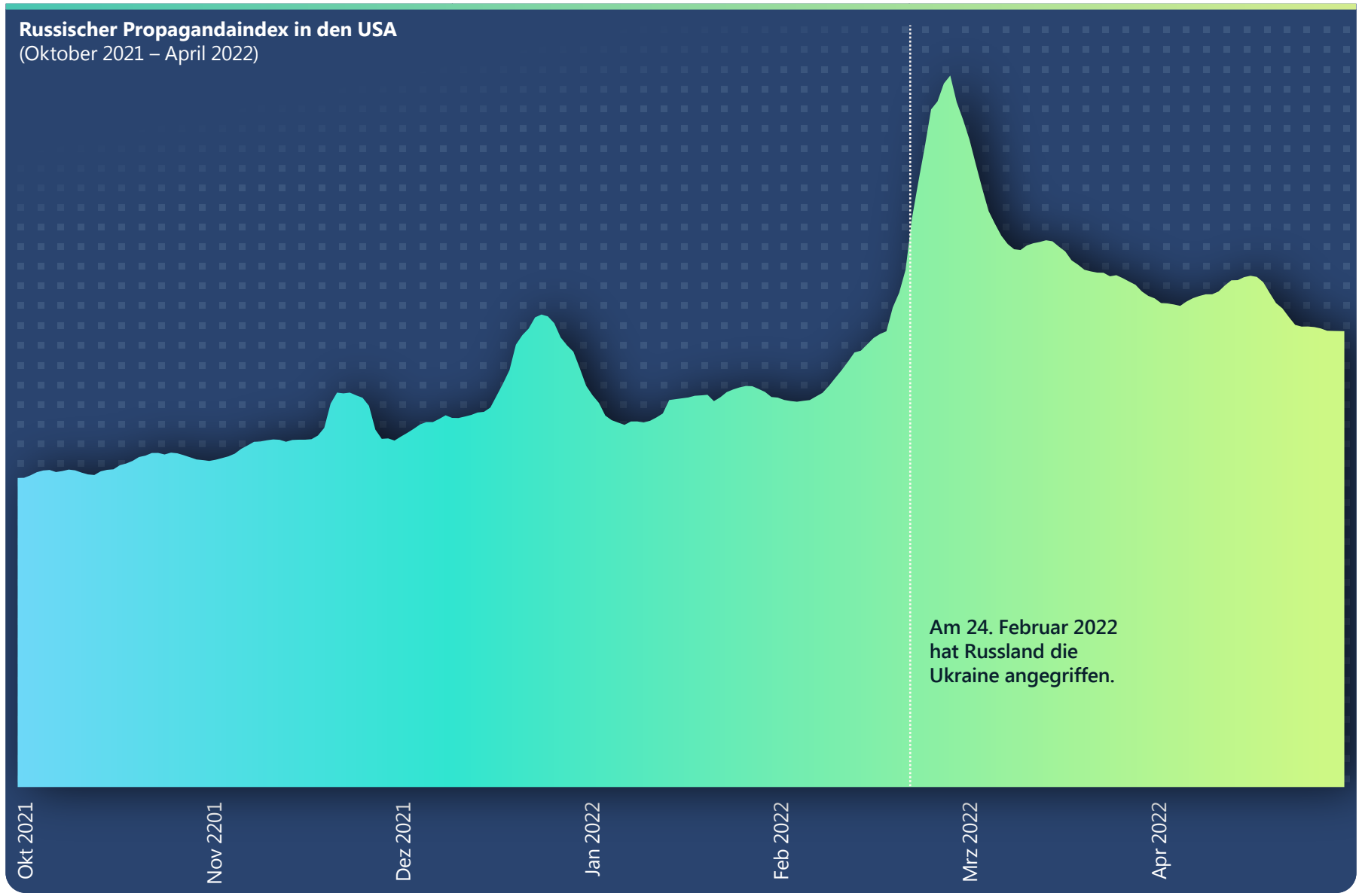
Links zu weiteren Informationen

- Defending Ukraine: Early Lessons from the Cyber War | Microsoft On the Issues
- An overview of Russia's cyberattack activity in Ukraine | Microsoft Special Report
- Disrupting cyberattacks targeting Ukraine | Microsoft On the Issues

Nachverfolgung des russischen Propagandaindex

Im Januar 2022 leiteten fast 1.000 US-Websites Datenverkehr auf russische Propagandawebsites weiter. Die häufigsten Themen für russische Propagandawebsites, die ein US-Publikum ansprachen, waren der Krieg in der Ukraine, die US-amerikanische Innenpolitik (entweder pro Trump oder pro Biden) und COVID-19 sowie impfstoffbezogene Narrative.

Der russische Propagandaindex (RPI) überwacht den Fluss von Nachrichten aus staatlich kontrollierten und gesponserten russischen Nachrichtenagenturen und Verstärkern als Anteil des gesamten Nachrichten-Traffics im Internet. Mit dem RPI lässt sich der Konsum russischer Propaganda für das ganze Internet und in verschiedenen Regionen auf einer präzisen Zeitleiste darstellen. Zu beachten ist hierbei, dass Microsoft nur die russische Propaganda beobachten kann, die auf zuvor identifizierten Websites gepostet wird. Wir haben keinen Einblick in Propaganda auf anderen Arten von Websites. Das umfasst auch maßgebliche neue Nachrichtenwebsites, nicht identifizierte Websites und Gruppen in sozialen Netzwerken.



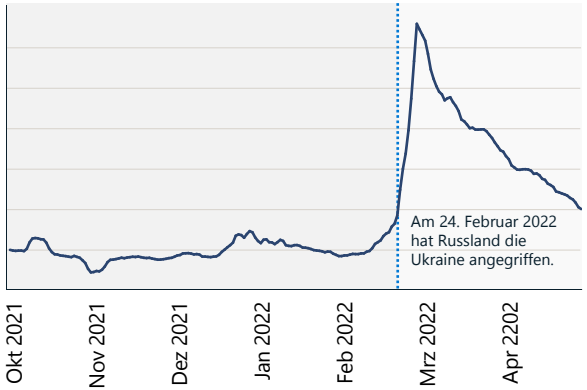
Nachverfolgung des russischen Propagandaindex

Fortsetzung

Russischer Propagandaindex: Ukraine

Als der Ukrainekrieg begann, stieg die russische Propaganda um 216 % und erreichte am 2. März ihren Höhepunkt. Die folgende Grafik zeigt, wie diese plötzliche Zunahme mit dem Beginn des Angriffskriegs zusammenfiel. Die beiden Graphen zeigen, wie die russische Propaganda kurz nach Beginn der kriegerischen Handlungen stark zugenommen hat.

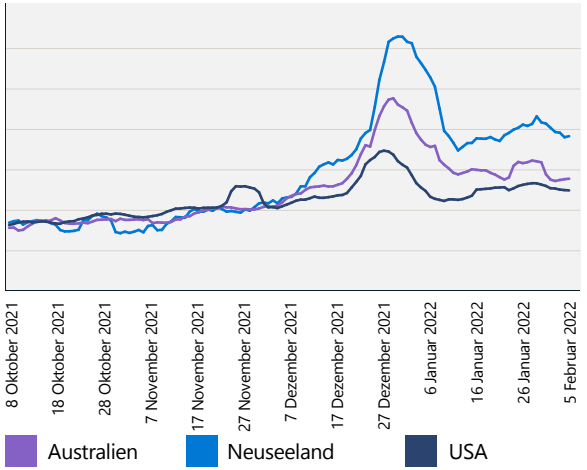
RPI, Ukraine
(7. Oktober 2021 – 30. April 2022)



Russischer Propagandaindex: Neuseeland im Vergleich mit Australien und den USA

Eine Auswertung des RPI in Neuseeland zeigte Ende 2021 eine Spitze, die mit COVID-19-Propaganda zusammenhing. Diese Spitze beim Konsum russischer Propaganda in Neuseeland ging einer Zunahme der öffentlichen Proteste Anfang 2022 in Wellington voran. Eine zweite Spitze stand eindeutig im Zusammenhang mit dem russischen Angriff auf die Ukraine und übertraf die RPIs Australiens und der USA.

RPI, Neuseeland im Vergleich mit Australien und den USA



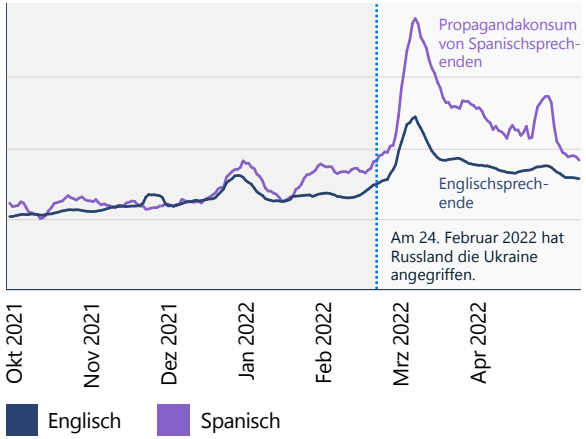
Bis zur ersten Dezemberwoche 2021 ähnelt der Konsum russischer Propaganda in Neuseeland dem Australiens. Nach Dezember stieg der Konsum russischer Propaganda in Neuseeland gegenüber dem in Australien und in den USA um mehr als 30 %.

Russischer Propagandaindex in den Vereinigten Staaten: Englisch und Spanisch

Die RPI verfolgt auch Propaganda in verschiedenen Sprachen. Mehrere Medien, einschließlich RT und Sputnik News, sind in mehr als 20 Sprachen verfügbar. Dazu gehören Englisch, Spanisch, Deutsch, Französisch, Griechisch, Italienisch, Tschechisch, Polnisch, Serbisch, Lettisch, Litauisch, Moldauisch, Weißrussisch, Armenisch, Ossetisch, Georgisch, Aserbaidschanisch, Arabisch, Türkisch, Persisch und Dari.

Die folgende Grafik zeigt, dass der RPI für spanischsprachige Nachrichten in den USA viel höher ist als für englischsprachige Nachrichten.

Der Konsum russischer Propaganda ist unter Spanisch Sprechenden 2x höher



Der Konsum russischer Propaganda ist in den USA unter Spanisch Sprechenden zweimal höher.

Russische Propaganda ist in Lateinamerika weit verbreitet

RT auf Spanisch ist das internationale Medium mit der höchsten Anzahl von Seitenaufrufen und Facebook-Followern.

Quelle: Microsoft AI for Good Research Lab

Synthetische Medien

Wir gehen in ein goldenes Zeitalter für KI-gesteuerte Medienerstellung und -manipulation. Analyst*innen von Microsoft stellen fest, dass dies von zwei wesentlichen Trends befeuert wird: der Verbreitung benutzungsfreundlicher Tools und Dienste für die künstliche Erstellung hoch realistischer synthetischer Bild-, Video-, Ton- und Textinhalte sowie der Fähigkeit, diese schnell und auf bestimmte Zielgruppen zugeschnitten zu verbreiten.

Keine dieser Entwicklungen ist für sich genommen problematisch. Mit KI-basierter Technologie lassen sich unterhaltsame und spannende digitale Inhalte erstellen, sei es rein synthetisch oder zur Ergänzung vorhandener Materialien. Diese Tools werden von Unternehmen weithin für Werbung und Kommunikation eingesetzt und von Einzelpersonen zum Erstellen ansprechender Inhalte für ihre Follower. Synthetische Medien haben jedoch das Potenzial, Einzelpersonen, Unternehmen, Institutionen und der Gesellschaft schweren Schaden zuzufügen, wenn sie mit böswilliger Absicht erstellt und verbreitet werden. Microsoft ist eine treibende Kraft hinter der Entwicklung von Technologien und Verfahren zum Begrenzen dieser Schäden – sowohl intern als auch in der ganzen breiteren Medieninfrastruktur.

Dieser Abschnitt geht auf Befunde aus Microsoft-Analysen zu den zurzeit modernsten Technologie zum Erstellen schädlicher synthetischer Inhalte ein, auf die Schäden, die eine weite Verbreitung dieser Inhalte anrichten kann, und auf die technischen Gegenmaßnahmen, die zur Abwehr von Cyberbedrohungen mit synthetischen Medien eingesetzt werden können.

Erstellen synthetischer Medien

Der Bereich der synthetischen Texte und Medien entwickelt sich unglaublich schnell weiter, weil Techniken, die einst nur mit den enormen Rechenressourcen großer Filmstudios möglich waren, jetzt in Smartphone-Apps integriert sind. Gleichzeitig werden die Tools immer einfacher zu bedienen und können Inhalte mit einem Grad von Realismus generieren, der sogar forensische Medienspezialist*innen täuschen kann. Wir stehen kurz davor, den Punkt zu erreichen, an dem jeder synthetische Videos erstellen kann, in denen jede beliebige Person etwas Beliebiges tut oder sagt. Es ist nicht unrealistisch, davon auszugehen, dass wir in eine Ära eintreten, in der ein erheblicher Anteil der Inhalte, die wir online sehen, vollständig oder teilweise synthetisch ist – erstellt mithilfe von KI-Techniken.

> Mit der Verfügbarkeit von komplexeren, aber dennoch benutzungsfreundlichen und weit verbreiteten Tools nimmt die Erstellung synthetischer Inhalte stetig zu, und diese werden schon bald nicht mehr von der Realität zu unterscheiden sein.

Es gibt viele hochwertige kostenlose und kommerzielle Tools zur Bild-, Video- und Audiobearbeitung. Mit diesen Tools lassen sich einfache, aber potenziell schädliche Änderungen an Inhalten vornehmen, etwa das Hinzufügen von irreführendem Text, das Austauschen von Gesichtern („Face Swapping“) und das Entfernen oder Ändern von Kontext. Solche „Cheap Fakes“ werden häufig verwendet, um schändliche Inhalte zu verbreiten, politische Ideologien zu unterstützen und Reputationen zu beschädigen. Ein bekanntes Beispiel ist ein Video aus dem Jahre 2019[16], in dem die Sprecherin des US-Repräsentantenhauses, Nancy Pelosi, undeutlich spricht und betrunken erscheint. Obwohl schnell klar war, dass das Video verlangsamt worden war, um diesen Effekt zu erzeugen, fand der Cheap Fake weite Verbreitung, bevor das Originalvideo in seinem ursprünglichen Kontext auftauchte.

Raffiniertere Herangehensweisen an das Manipulieren von Medieninhalten sind beispielsweise die Anwendung moderner, erweiterter KI-Techniken, um (a) rein synthetische Medien zu erstellen und (b) komplexere Bearbeitungen vorhandener Medien durchzuführen. Häufig wird der Begriff „Deepfake“ für solche synthetischen Medien verwendet, die mithilfe modernster KI-Techniken erstellt wurden (der Name stammt von den manchmal verwendeten „tiefen“ neuronalen Netzwerken). Diese Technologien werden als eigenständige Apps, Tools und Dienste entwickelt und in etablierte kommerzielle und Open Source-Bearbeitungstools integriert.

Solche Technologien werden von bösartigen Akteuren als Waffe eingesetzt mit dem Ziel, Personen und Institutionen zu beschädigen. Beispiele für Deepfake-Techniken sind:

- **Face Swap (Video, Bilder)** – Ersetzen eines Gesichts in einem Video durch ein anderes. Diese Technik lässt sich verwenden, um eine Person, ein Unternehmen oder eine Institution zu erpressen oder um Personen in peinlichen Orten oder Situationen zu zeigen.
- **Puppeteering (Video, Bilder)** – Verwendung eines Videos zum Animieren eines Standbilds oder anderen Videos. Dies kann den Eindruck erwecken, dass eine Person etwas Peinliches oder Irreführendes gesagt hat.
- **Generative Adversarial Networks (Video, Bilder)** – eine Gruppe von Techniken zum Erstellen fotorealistischer Bilder und Videos.
- **Transformer-Modelle (Video, Bilder, Text)** – Erstellen von umfangreichen Bildern aus Textbeschreibungen.

Solche fortschrittlichen KI-basierten Techniken sind heute noch nicht weit verbreitet, aber wir erwarten, dass das Problem zunehmen wird, weil die Tools immer einfacher zu verwenden sind und immer weitere Verbreitung finden.

Die Auswirkungen von Manipulation mit synthetischen Medien

Die Verwendung von Informationsprozessen, um Schaden anzurichten oder Einfluss zu nehmen, ist nicht neu. Die Geschwindigkeit, mit der Informationen verbreitet werden können, und unsere Unfähigkeit, Fakten und Fiktion schnell unterscheiden zu können, bedeutet, dass die Auswirkungen und die Schäden von und durch Fälschungen („Fakes“) und andere synthetisch hergestellte bösartige Medien viel größer ausfallen können als es beispielsweise beim Beispiel mit Nancy Pelosi der Fall war.

Wir berücksichtigen mehrere Kategorien von Schäden: Marktmanipulation, Zahlungsbetrug, Vishing, Identitätswechsel, Markenschäden, Reputationsschäden und Botnets. Für viele dieser Kategorien gibt es weithin gemeldete praktische Beispiele, die unsere Fähigkeit, Fakten und Fiktion auseinanderzuhalten, untergraben könnten.

Wenn wir dem, was wir sehen und hören, nicht mehr vertrauen können, ist das eine längerfristige und heimtückischere Bedrohung für unser Verständnis von Wahrheit. Aus diesem Grund kann jedes kompromittierende Bild-, Ton- oder Videodokument einer öffentlichen oder privaten Person als Fake abgetan werden. Dieser Effekt wird als „The Liar's Dividend“[17] (zu Deutsch etwa „Die Lügnerdividende“) bezeichnet. Aktuelle Forschung[18] zeigt, dass dieser Technologiemissbrauch bei Angriffen auf Finanzsysteme bereits verwendet wird. Allerdings sind auch weitere Missbrauchsszenarien plausibel.

Synthetische Medien

Fortsetzung

Erkennen synthetischer Medien

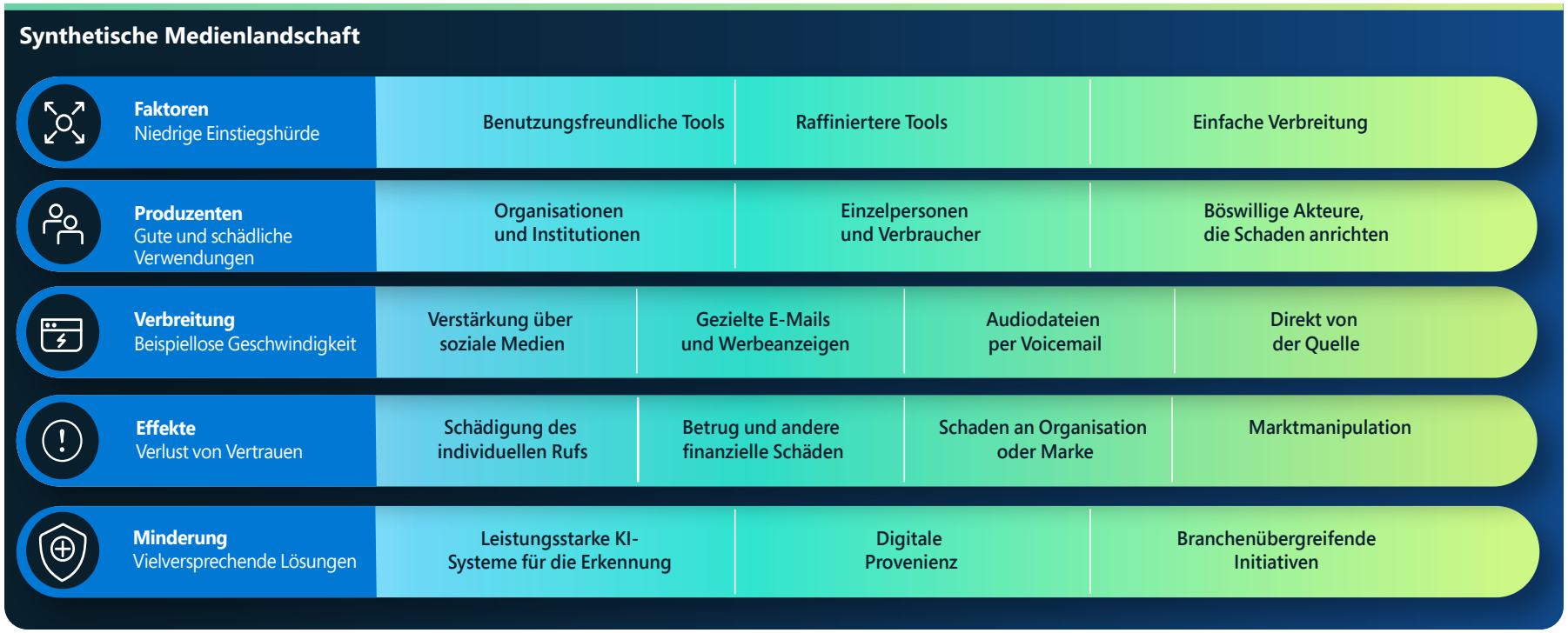
Die Industrie, staatliche Einrichtungen und die akademische Welt unternehmen gemeinsam Anstrengungen, um bessere Methoden zum Aufspüren und Eindämmen synthetischer Medien zu finden und das Vertrauen wiederherzustellen. Es gibt mehrere vielversprechende Wege in die Zukunft, aber auch Hindernisse, die berücksichtigt werden müssen.

Ein Ansatz besteht in der Entwicklung KI-gestützter Systeme, die Fälschungen erkennen können – im Wesentlichen „defensive" KI-Systeme zur Bekämpfung der „offensiven" KI-Systeme. Dies ist ein Bereich der aktiven Forschung, in dem aktuelle Systeme zum Erstellen synthetischer Audio- oder Videodateien verräterische Artefakte hinterlassen, die von entsprechend geschulten forensischen Analyst*innen und automatisierten Tools erkannt werden können.

Während aktuelle Fälschungen verräterische Mängel aufweisen, hängen die genauen Artefakte eher von dem jeweils verwendeten Tool oder Algorithmus ab. Das bedeutet, dass Trainings zu bekannten Fälschungen normalerweise nicht allgemein auf andere Algorithmen übertragen werden können. Dies zeigte sich bei einem offenen Wettbewerb im Jahr 2020, bei dem es darum ging, Detektoren für Deepfake-Bilder zu entwickeln.[19] Auch wenn es verlockend ist, mehr in die Entwicklung noch besserer Detektoren zu investieren, ist Microsoft sehr skeptisch, dass dies zu nennenswerten Resultaten führen wird, und zwar aus zwei Gründen:

Erstens haben wir ausgezeichnete physische Modelle, die die reale Welt widerspiegeln. Aktuelle Entwickler*innen von Fälschungen nehmen gerne Abkürzungen. Dies führt zu Artefakten, die sich aufspüren lassen. Neuere Modelle werden jedoch immer realistischer. An sich gibt es nichts Besonderes an der Fotografie einer realen Szene, das nicht von einem Computer modelliert werden könnte.

Zweitens verwenden moderne Algorithmen zur Erstellung der Fälschungen eine Technik namens Generative Adversarial Networks (GANs). Ein GAN spielt zwei KI-Systeme gegeneinander aus: Es erstellt die Fälschung über einen Generator und nutzt einen Diskriminator, um falsche Bilder zu erkennen und den Generator zu trainieren. Jede Investition in die Entwicklung eines besseren Detektors lässt den Generator nur noch bessere Fälschungen erstellen.



Synthetische Medien

Fortsetzung

Provenienz für digitale Ressourcen

Doch was lässt sich tun, um sich vor der schädlichen Nutzung synthetischer Medien zu schützen, wenn das Aufspüren von Fälschungen so unzuverlässig ist? Eine wichtige neue Technologie ist die sogenannte digitale Provenienz: ein Mechanismus, mit dem Urheber*innen von digitalen Medien eine Ressource zertifizieren und Kund*innen manipulierte digitale Ressourcen erkennen können. Im Kontext der heutigen Social Media-Netzwerke, über die sich Inhalte rasant im Internet verbreiten und bösartige Akteure die Gelegenheit erhalten, Inhalte ohne großen Aufwand zu manipulieren, ist digitale Provenienz besonders wichtig.

900 %

Zunahme bei der Verbreitung von Deepfakes seit 2019.[20]

Bei der Technologie der digitalen Provenienz handelt es sich um eine moderne Version kryptografischer Signaturen von Dokumenten. Sie wurde entwickelt, um die Quelle, die Bearbeitungshistorie und die Metadaten von Objekten auf ihrem Weg durch das heutige Internet zu erfassen. Die Vision und die technischen Verfahren, die eine solche durchgängig manipulationssichere Zertifizierung von Medien möglich machten, wurden von einem interdisziplinären Team aus Forschenden und Wissenschaftler*innen bei Microsoft entwickelt. Gemeinsam mit anderen führen wir eine branchenübergreifende Partnerschaft an, um die Technologie zur Medienprovenienz im Rahmen von Project Origin (gegründet von Microsoft, der BBC, CBC/Radio-Canada und der New York Times) zum Leben zu erwecken, und wir engagieren uns in der Content Authenticity Initiative (gegründet von Adobe). Zusammen mit Technologie- und Medienpartnern etablierte Microsoft außerdem die Coalition for Content Provenance and Authenticity (C2PA). C2PA ist eine Normungsorganisation, die vor kurzem die bisher weitestgehende Spezifikation für digitale Provenienz veröffentlicht hat. Sie kann für Medienressourcen wie Bild-, Video-, Audio- und Textdateien herangezogen werden.

Ein C2PA-kompatibles Objekt enthält ein Manifest, das das Objekt und die Metadaten vor Manipulationen schützt. Das zugehörige Zertifikat identifiziert den Herausgeber.

Synthetische Medien waren ursprünglich nicht darauf ausgelegt, Schäden anzurichten. Allerdings werden sie gerade zu Waffen umfunktioniert, um das Vertrauen in Einzelpersonen und Institutionen zu untergraben.

Digitale Provenienz ist eine vielversprechende aufstrebende Technologie, die das Potenzial hat, das Vertrauen der Menschen in die Inhalte von Onlinemedien durch eine Zertifizierung des Ursprungs der Medienressource wiederherzustellen.

Öffentlich verfügbare Lösungen, die auf der C2PA-Spezifikation basieren, werden entweder als neue Funktion in vorhandenen Produkten oder als neue Standalone-Apps und -Dienste in Erscheinung treten. Wir erwarten, dass die meisten gängigen Tools für die Erfassung, Bearbeitung und Erstellung von Inhalten in einigen Jahren C2PA-kompatibel sein werden. Dies bietet Unternehmen die Möglichkeit, ihre Anforderungen und Anwendungen für die digitale Provenienz schon heute zu ermitteln und diese zusätzliche Schutzebene für die Tools einzufordern, die sie in ihren vorhandenen Workflows verwenden.

Umsetzbare Insights

1. Ergreifen Sie Schritte, um Ihr Unternehmen vor Fehlinformationen zu schützen, indem Sie proaktiv Reaktionen für PR und Kommunikation entwickeln.
2. Nutzen Sie die Provenienz-Technologie, um die offizielle Kommunikation zu schützen.

Links zu weiteren Informationen

- A promising step forward on disinformation | Microsoft On the Issues
- A Milestone Reached, 31. Januar 2022
- Project Origin | Microsoft ALT Innovation
- Coalition for Content Provenance and Authenticity (C2PA)
- Explore technical details about the system Project Origin uses for media authentication | Microsoft ALT Innovation

Ein ganzheitlicher Ansatz zum Schutz vor Operationen zur Einflussnahme im Cyberspace

Microsoft baut auf der bereits ausgereiften Cyber Threat Intelligence-Infrastruktur auf, um einen umfassenderen und integrativeren Überblick über Operationen zur Einflussnahme im Cyberspace zu gewinnen.

Wir nutzen ein Framework für empfohlene Reaktions- und Abwehrstrategien, um die Bedrohung durch solche Operationen zu bekämpfen. Diese Strategien lassen sich im Wesentlichen in vier Säulen unterteilen: Entdecken, Unterbinden, Abwehren und Abschrecken.

Darüber hinaus hat Microsoft vier Prinzipien eingeführt, um unsere Arbeit in diesem Bereich zu verankern. Das erste ist die Verpflichtung, die Meinungsfreiheit zu respektieren sowie die Fähigkeit unserer Kunden zu wahren, Informationen mithilfe unsere Plattformen, Produkte und Dienste zu erstellen, zu veröffentlichen und zu suchen. Zweitens arbeiten wir proaktiv daran zu verhindern, dass unsere Plattformen und Produkte zur Verstärkung ausländischer Seiten und Inhalte für die Einflussnahme im Cyberspace genutzt werden. Drittens werden wir nicht vorsätzlich von Inhalten oder Akteuren, die auf eine Einflussnahme im Cyberspace abzielen, profitieren. Schließlich priorisieren wir die auftauchenden Inhalte, um ausländischen Operationen zur Einflussnahme im Cyberspace durch Nutzung interner Daten sowie vertrauenswürdiger Daten von Dritten in unseren Produkten entgegenzuwirken.

Entdecken

Wie bei der Cyberverteidigung besteht der erste Schritt bei der Abwehr von Operationen zur Einflussnahme im Cyberspace darin, die Fähigkeit zu entwickeln, sie überhaupt zu erkennen. Kein einzelnes Unternehmen und keine einzelne Organisation kann darauf hoffen, den erforderlichen Fortschritt alleine zu erreichen. Eine neue, breitere Zusammenarbeit, die den gesamten Technologiesektor umspannt, wird entscheidend sein. Dabei hängt der Fortschritt bei der Analyse und dem Meldewesen von Operationen zur Einflussnahme im Cyberspace stark von der Rolle der Zivilgesellschaft ab, einschließlich akademischer Einrichtungen und gemeinnütziger Organisationen.

In Anerkennung dieser Rolle haben die Forschenden Jake Shapiro und Alicia Wanless an der Princeton University und des Carnegie Endowment for International Peace bereits Pläne für den Start des neuen „Institute for Research on the Information Environment" (IRIE) vorgestellt. Mit Unterstützung von Microsoft, der Knight Foundation und Craig Newmark Philanthropies wird das IRIE eine integrative, mehrere Interessengruppen umfassende Forschungseinrichtung nach dem Vorbild des europäischen Kernforschungszentrums CERN erschaffen. Es kombiniert Fachwissen in der Datenverarbeitung mit Expertise in der Datenanalyse, um so neue Entdeckungen in diesem Bereich zu beschleunigen und auszuweiten. Politische Entscheidungsträger*innen, Technologieunternehmen und, im weiteren Sinne, die Verbraucher*innen werden umfassend über die Ergebnisse informiert.

Abwehren

Die zweite strategische Säule besteht im Absichern demokratischer Verteidigungsmaßnahmen – eine langjährige Priorität, die Investitionen und Innovation bedarf. Dabei müssen die Herausforderungen berücksichtigt werden, die Technologie für die Demokratie geschaffen hat, aber auch die Möglichkeiten, die durch sie entstanden sind, um demokratische Gesellschaften noch effektiver verteidigen zu können.

Das Strategieframework von Microsoft zielt darauf ab, sektorübergreifenden Interessengruppen beim Erkennen, Unterbinden, Abwehren und Abschrecken von Propaganda zu helfen. Dabei geht es im besonderen Maße um Kampagnen von ausländischen Aggressoren.

Es ist angebracht, mit einer der großen technologischen Herausforderungen unserer Zeit zu beginnen – den Folgen des Internets und der digitalen Werbung für den traditionellen Journalismus. Seit dem 18. Jahrhundert hat eine freie und unabhängige Presse eine besondere Rolle bei der Unterstützung jeder Demokratie auf der Welt gespielt – durch das Aufdecken von Korruption, das Dokumentieren von Kriegen und das Beleuchten der größten gesellschaftlichen Herausforderungen dieser und jeder anderen Zeit. Allerdings hat das Internet lokalen Medienhäusern schwer zugesetzt, weil es Werbeeinnahmen verschlingt und zahlende Abonnenten weglockt. Viele lokale Zeitungen sind zusammengebrochen. Eine der vielen Erkenntnisse aus unserer jüngsten Arbeit ist, dass Städte, die keine Zeitung haben, unwissentlich und zwangsläufig einem überdurchschnittlichen Volumen ausländischer Propaganda ausgesetzt sind. Aus diesen Gründen besteht eine der wichtigsten Verteidigungslinien einer Demokratie im Stärken des traditionellen Journalismus und der freien Presse – gerade auf lokaler Ebene. Dazu bedarf es fortlaufender Investitionen und Innovationen, die die lokalen Bedürfnisse verschiedener Länder und Kontinente widerspiegeln. Diese Probleme sind nicht einfach und erfordern Herangehensweisen, die mehrere Interessengruppen einbinden und die von Microsoft und anderen Technologieunternehmen zunehmend unterstützt werden.

Wir brauchen auch Innovationen für die öffentliche Ordnung. Das muss eine zivilgesellschaftliche Priorität sein. Dies kann Gesetze umfassen, die Verlage in die Lage versetzen, Werbeeinnahmen gemeinsam mit Technologieunternehmen auszuhandeln, und eine Gesetzgebung, die Steuererleichterungen für Lokalredaktionen vorsieht, um sie von einem Teil der Lohnsteuer für ihre angestellten Journalisten zu entlasten. Journalisten brauchen für ihr Handwerk noch viele weitere Tools. Dazu gehört auch die Fähigkeit, Inhalte von betrügerischen Quellen von solchen aus legitimen zu unterscheiden.

Es gibt auch einen schnell wachsenden Bedarf dafür, Kund*innen dabei zu helfen, eine ausgeprägte Fähigkeit zum Erkennen von nationalstaatlich finanzierten Informationskampagnen zu entwickeln. Die Aufgabe mag gewaltig erscheinen, aber es erinnert an die Arbeit, die der Technologiesektor bei der Bekämpfung anderer Cyberbedrohungen schon lange leistet. Denken Sie beispielsweise an die Aufklärung der Verbraucher*innen, dass sie genauer auf eine E-Mail-Adresse achten sollten, um Spam oder andere betrügerische Nachrichten leichter zu erkennen. Initiativen in den USA – wie das News Literacy Project und das Trusted Journalism

Wenn wir dem, was wir sehen und hören, nicht mehr vertrauen können, ist das eine längerfristige und heimtückischere Bedrohung für unser Verständnis von Wahrheit.

Ein ganzheitlicher Ansatz zum Schutz vor Operationen zur Einflussnahme im Cyberspace

Fortsetzung

Program – tragen dazu bei, eine besser informierte Verbraucherschaft von Nachrichten und Informationen zu schaffen. Weltweit können neue Technologien wie das Browser-Plugin von NewsGuard dieses Vorhaben noch deutlich beschleunigen.

Dies sollte uns auch daran erinnern, dass ein Unterricht in Staatsbürgerkunde eine wichtige Säule der Demokratie bildet. Wie immer muss dieses Vorhaben in den Schulen beginnen. Wir leben jedoch in einer Welt, die erfordert, dass wir alle im Laufe unseres Lebens laufend in Staatsbürgerkunde geschult werden. Die neue „Civics at Work"-Initiative, deren Mitbegründer und Partner Microsoft ist und die vom Center for Strategic and International Studies geleitet wird, will die Inhalte der Staatsbürgerkunde innerhalb der Unternehmenscommunitys zu neuem Leben erwecken. Es ist ein gutes Beispiel dafür, wie breit gefächert die Möglichkeiten sind, die uns bei der Verteidigung unserer Demokratie stärker machen können.

Unterbinden

In den letzten Jahren hat die Digital Crimes Unit (DCU) von Microsoft ausgefeilte Taktiken und Tools zur Abwehr von Cyberbedrohungen entwickelt, die von Ransomware über Botnets bis hin zu nationalstaatlichen Angriffen reichen. Wir haben viele wichtige Lektionen gelernt, angefangen bei der Rolle des aktiven Unterbindens bei der Abwehr einer breiten Palette von Cyberangriffen.

Beim Bekämpfen von Operationen zur Einflussnahme im Cyberspace spielt das Unterbinden womöglich eine noch wichtigere Rolle, und langsam wird klar, wie die beste Herangehensweise aussehen muss. Das wirksamste Gegenmittel gegen umfangreiche Täuschung ist Transparenz. Darum hat Microsoft durch die Übernahme von Miburo Solutions seine Kapazitäten zum Erkennen und Unterbinden von nationalstaatlichen Beeinflussungsoperationen erweitert. Dabei handelt es sich um ein führendes Unternehmen bei der Analyse und Erforschung von Cyberbedrohungen, das auf die Erkennung und Bekämpfung von ausländischen Operationen zur Einflussnahme im Cyberspace spezialisiert ist.

Unsere Erfahrung hat gezeigt, dass staatliche Einrichtungen, Technologieunternehmen und NGOs bei der Zuschreibung von Cyberangriffen sorgfältig und mit ausreichend Beweisen vorgehen sollten. Es ist enorm wichtig, die Auswirkungen solcher störenden Eingriffe zu verstehen. Dies kann beim Unterbinden von Einflussnahmen im Cyberspace sogar noch hilfreicher sein. Zeugnis dafür ist die Informationsweitergabe der US-Regierung im Vorfeld des russischen Angriffskriegs gegen die Ukraine. Dabei wurde Transparenz mit großer Wirkung angewendet, z. B. beim Offenlegen russischer Pläne, einschließlich spezifischer Kampagnen wie ein Komplott zum Einsatz eines gefälschten expliziten Videos.

Wie die Veröffentlichung des CyberPeace Institute in Genf im vergangenen Sommer zeigt, die sich mit laufenden Cyberangriffen innerhalb und außerhalb der Ukraine beschäftigt hat, besteht eine Chance für eine breite Palette von Organisationen der Zivilgesellschaft und des privaten Sektors, die Transparenz in Bezug auf Operationen zur Einflussnahme im Cyberspace zu fördern. Zuverlässige Berichte über neu entdeckte und gut dokumentierte Operationen können der Öffentlichkeit helfen, besser zu bewerten, was sie liest, sieht und hört, insbesondere im Internet. Zu diesem Zweck wird Microsoft auf vorhandenen Cyberberichten aufbauen, diese weiterentwickeln und außerdem neue Berichte, Daten und Updates im Zusammenhang mit unseren Erkenntnissen über Operationen zur Einflussnahme im Cyberspace veröffentlichen. Dies umfasst ggf. auch Aussagen zur Zuschreibung. Wir werden einen jährlichen Bericht herausgeben, der mit einer datengestützten Herangehensweise einen unternehmensweiten Blick auf die Prävalenz ausländischer Informationsoperationen wirft sowie auf die nächsten Schritte zum Sicherstellen einer inkrementellen Verbesserung. Wir werden auch zusätzliche Schritte in Betracht ziehen, die auf dieser Art von Transparenz aufbauen.

Zum Beispiel ist die Rolle digitaler Werbung besonders wichtig, weil Werbung bei der Finanzierung ausländischer Operationen helfen kann und gleichzeitig vom Ausland finanzierten Propagandaseiten einen legitimen Anstrich gibt. Zum Unterbrechen dieser Finanzströme werden neue Initiativen nötig sein.

Abschrecken

Wir können von Nationen nicht erwarten, ihr Verhalten zu ändern, wenn jene, die internationale Regeln verletzen, nicht zur Verantwortung gezogen werden. Die Durchsetzung dieser Rechenschaftspflicht liegt einzig und allein in der Verantwortung von Regierungen. Trotzdem spielen koordinierte Aktionen mehrerer Interessengruppen eine zunehmend wichtige Rolle beim Stärken und Erweitern internationaler Normen. Mehr als 30 Onlineplattformen, Inserenten und Publisher – darunter auch Microsoft – unterzeichneten den kürzlich aktualisierten Verhaltenskodex zur Desinformation der Europäischen Kommission und stimmten damit zu, ihren Einsatz bei der Bekämpfung dieser wachsenden Herausforderung noch zu verstärken. Wie der kürzliche Aufruf von Paris, der Aufruf von Christchurch und die Erklärung zur Zukunft des Internets können multilaterale und von mehreren Interessengruppen getragene Maßnahmen die Regierungen und die Öffentlichkeit der demokratischen Nationen zusammenbringen. Staatliche Einrichtungen können dann auf diesen Normen und Gesetzen aufbauen, um die Rechenschaftspflicht voranzubringen, die die Demokratien der Welt brauchen und verdienen.

Durch schnelle, radikale Transparenz können demokratische Regierungen und Gesellschaften Beeinflussungskampagnen wirksam entschärfen. Dazu nehmen sie eine klare Zuschreibung der Quelle des nationalstaatlichen Angriffs vor, informieren die Öffentlichkeit und bauen Vertrauen in die Institutionen auf.

> Wir haben die technische Kapazität zum Erkennen und Unterbinden von ausländischen Beeinflussungsoperationen erhöht und verpflichten uns zu einer transparenten Berichterstattung über diese Operationen – wie schon in unseren Berichten über Cyberangriffe.

Umsetzbare Insights

1. Implementieren Sie starke digitale Hygieneverfahren in Ihrer gesamten Organisation.
2. Überlegen Sie, wie Sie jegliches unbeabsichtigte Ermöglichen von Kampagnen zur Einflussnahme im Cyberspace durch Ihre Mitarbeiter*innen oder durch Ihre Betriebspraktiken reduzieren können. Dazu gehört auch die Einschränkung des Angebots an bekannten ausländischen Propagandaseiten.
3. Unterstützen Sie Kampagnen für Informations- und Medienkompetenz und staatsbürgerliches Engagement als eine wichtige Komponente, um Gesellschaften bei der Verteidigung gegen Propaganda und ausländischen Einfluss zu helfen.
4. Setzen Sie sich direkt mit den Gruppen zusammen, die für Ihre Branche maßgeblich sind, um daran zu arbeiten, Beeinflussungsoperationen entgegenzuwirken.

Fußnoten

1. https://mitsloan.mit.edu/ideas-made-to-matter/mit-sloan-research-about-social-media-misinformation-and-elections?msclkid=8dc75d6abcfe11ecad9946a058d581c9
2. https://news.gallup.com/poll/355526/americans-trust-media-dips-second-lowest-record.aspx
3. Defending Ukraine: Early Lessons from the Cyber War (microsoft.com)
4. https://www.edelman.com/sites/g/files/aatuss191/files/2022-01/2022 Edelman Trust Barometer_FullReport.pdf
5. Sprecherin des russischen Außenministeriums Maria Sacharowa: https://tass.com/politics/1401777; Lavrov: https://www.cnn.com/2022/05/05/opinions/sergey-lavrov-hitler-comments-ukraine-kauders/index.html,Kirill Kudryavtsev/Pool/AFP/Getty Images
6. https://apnews.com/article/conspiracy-theories-iran-only-on-ap-media-misinformation-bfca6d5b236a29d61c4dd38702495ffe
7. https://www.justice.gov/opa/pr/united-states-seizes-websites-used-iranian-islamic-radio-and-television-union-and-kata-ib
8. https://www.presstv.ir/Detail/2020/02/04/617877/Is-the-coronavirus-a-US-bioweapon
9. https://www.state.gov/wp-content/uploads/2022/01/Kremlin-Funded-Media_January_update-19.pdf
10. https://www.rt.com/news/482405-iran-coronavirus-us-biological-weapon/
11. https://web.archive.org/web/20220319124125/https://twitter.com/RT_com/status/1233187558793924608?s=20
12. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd
13. Russia's Kremenchuk Claims Versus the Evidence – bellingcat
14. https://t.me/oddr_info/39658
15. https://t.me/voenacher/23339
16. Fact check: „Drunk" Nancy Pelosi video is manipulated | Reuters
17. https://lawcat.berkeley.edu/record/1136469
18. https://carnegieendowment.org/2020/07/08/deepfakes-and-synthetic-media-in-financial-system-assessing-threat-scenarios-pub-82237
19. Deepfake Detection Challenge Results: An open initiative to advance AI (facebook.com)
20. Deepfakes 2020: The Tipping Point, Johannes Tammekänd, John Thomas und Kristjan Peterson, Oktober 2020

Cyberresilienz

Das Verständnis der Risiken und Chancen von Modernisierung wird entscheidend für eine ganzheitliche Herangehensweise an das Thema der Resilienz.

Übersicht über

Cyberresilienz

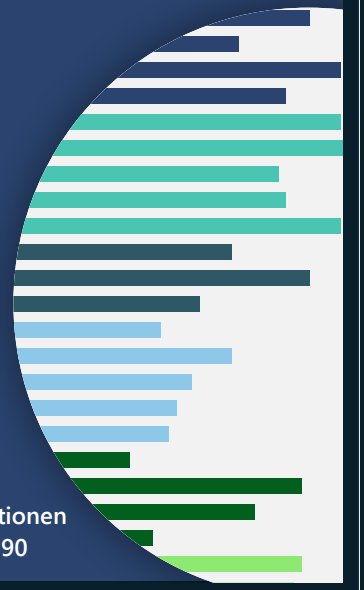
Cybersicherheit ist ein wichtiger Faktor für technologischen Erfolg. Innovation und gesteigerte Produktivität lassen sich nur durch die Einführung von Sicherheitsmaßnahmen erreichen, mit denen Unternehmen gegen moderne Angriffe so resilient wie möglich werden.

Die Pandemie hat uns vor die Herausforderung gestellt, unsere Sicherheitsmethoden und -technologien neu auszurichten, um die Mitarbeiter*innen von Microsoft zu schützen, egal, wo sie tätig sind. In diesem vergangenen Jahr haben Akteure weiterhin die während der Pandemie und des Umstiegs auf eine hybride Arbeitsumgebung zutage getretenen Schwachstellen ausgenutzt. Seitdem liegt unsere Herausforderung in erster Linie darin, auf die Verbreitung und Komplexität verschiedener Angriffsmethoden und die verstärkte Aktivität von Nationalstaaten zu reagieren.

Effektive Cyberresilienz erfordert einen ganzheitlichen, anpassungsfähigen Ansatz, um den sich entwickelnden Bedrohungen für zentrale Dienste und Infrastruktur standzuhalten.

Weitere Informationen finden Sie auf S. 89

Modernisierte Systeme und Architekturen sind wichtig für den Umgang mit Bedrohungen in einer vernetzten Welt.

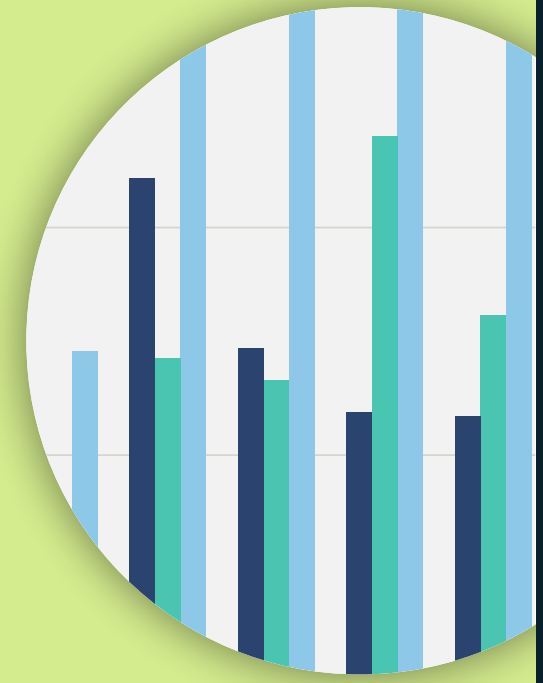


Weitere Informationen finden Sie auf S. 90

Der grundlegende Sicherheitsstatus ist ein entscheidender Faktor für mehr Lösungseffizienz.

Weitere Informationen finden Sie auf S. 92

Während kennwortbasierte Angriffe die Hauptquelle für die Kompromittierung von Identitäten bleiben, kommen weitere Angriffsarten hinzu.



Weitere Informationen finden Sie auf S. 93

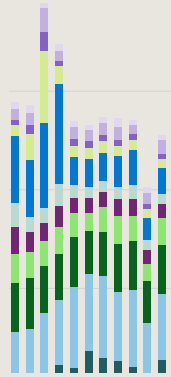
Die menschliche Dimension von Resilienz gegenüber Operationen zur Einflussnahme im Cyberspace ist unsere Fähigkeit zur Zusammenarbeit.

Weitere Informationen finden Sie auf S. 102

Die überwiegende Mehrheit der erfolgreichen Cyberangriffe könnte durch die Anwendung grundlegender Maßnahmen für die Sicherheitshygiene verhindert werden.

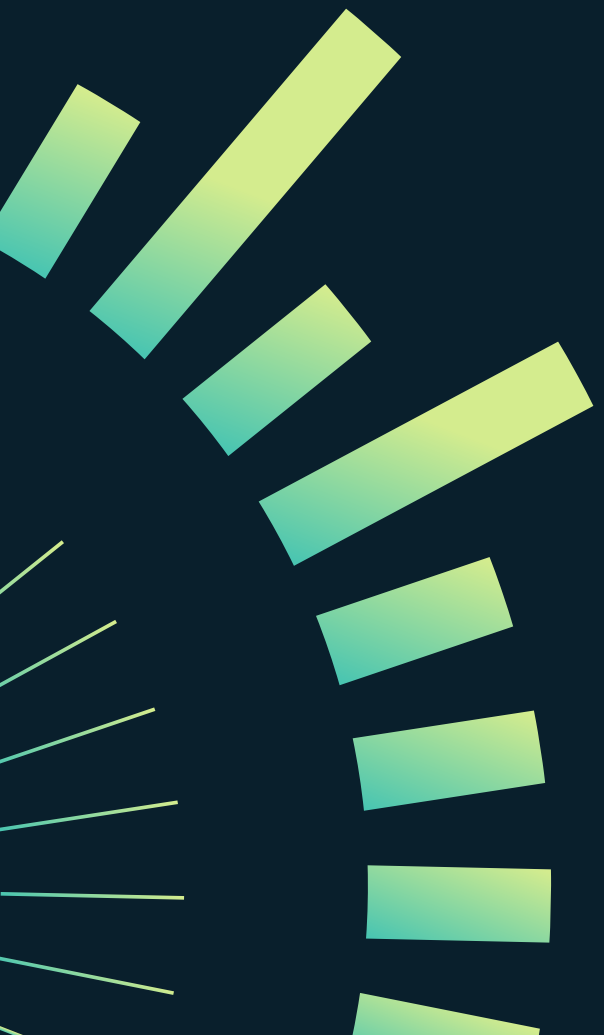
Weitere Informationen finden Sie auf S. 108

Im letzten Jahr erlebte die Welt eine DDoS-Aktivität, die in Bezug auf Volumen, Komplexität und Häufigkeit beispiellos war.



Weitere Informationen finden Sie auf S. 98

Einführung



Die Pandemie hat uns vor die Herausforderung gestellt, unsere Sicherheitsmethoden und -technologien neu auszurichten, um die Mitarbeiter*innen von Microsoft zu schützen, egal, wo sie tätig sind. In diesem vergangenen Jahr haben Akteure weiterhin die während der Pandemie und des Umstiegs auf eine hybride Arbeitsumgebung zutage getretenen Schwachstellen ausgenutzt. Seitdem liegt unsere Herausforderung in erster Linie darin, auf die Verbreitung und Komplexität verschiedener Angriffsmethoden und die verstärkte Aktivität von Nationalstaaten zu reagieren.

Die Aktivität globaler Bedrohungen befindet sich auf einem historischen Höchststand, und die Komplexität von Cyberangriffen wird jeden Tag höher. Viele der komplexen Angriffe von heute konzentrieren sich auf die Kompromittierung von Identitätsarchitekturen, Lieferketten und Drittanbietern mit unterschiedlichen Stufen von Sicherheitskontrollen. Insbesondere haben wir festgestellt, dass Angriffe zum Identitäts-Phishing eine eindeutige Bedrohung darstellen. Bei guten Verfahren für Identitätsverwaltung, Phishing-Kontrolle und Endpunktverwaltung bleiben Angriffe dieser Art jedoch in der Regel erfolglos. Daher müssen wir uns an die Grundlagen erinnern: 98 % der Angriffe können mit grundlegenden Hygienemaßnahmen gestoppt werden. Bei Microsoft verwalten wir Identitäten und Geräte im Einklang mit unserem Zero Trust-Ansatz. Dies umfasst Zugriff mit den geringstmöglichen Berechtigungen und Phishing-resistente Anmeldeinformationen, um Akteure wirksam zu stoppen und unsere Daten zu schützen.

Heute können selbst Akteure, denen es an ausgefeilten technischen Fähigkeiten mangelt, unglaublich zerstörerische Angriffe starten, weil der Zugang zu fortschrittlichen Taktiken, Techniken und Verfahren in der kriminellen Cyberwirtschaft umfassend verfügbar ist. Der Krieg in der Ukraine hat gezeigt, wie nationalstaatliche Akteure ihre offensiven Cyberoperationen über eine verstärkte Nutzung von Ransomware eskaliert haben. Ransomware ist inzwischen zu einer komplexen Branche geworden, in der Akteure Taktiken mit zweifacher oder dreifacher Erpressung anwenden, um eine Zahlung zu erzwingen, und Entwickler RaaS (Ransomware-as-a-Service) anbieten. Mit RaaS greifen Akteure zum Durchführen von Angriffen auf ein Affiliate-Netzwerk zurück. Dies senkt die Zugangshürden für weniger kompetente Cyberkriminelle und erweitert, in letzter Konsequenz, den Pool der Angreifer.

Daher hat Microsoft ein Programm zur Eliminierung von Ransomware entwickelt. Das Ziel des Programms besteht darin, Lücken bei Kontrollen und Abdeckung zu beseitigen, zu Funktionsverbesserungen von Diensten beizutragen und Wiederherstellungs-Playbooks für unsere Sicherheits- und Entwicklungsteams im Falle eines Ransomware-Angriffs zu entwickeln.

Die jüngsten Angriffe auf Lieferketten und Drittanbieter deuten auf einen wichtigen Wendepunkt in der Branche hin. Die Verwerfungen, die diese Angriffe für unsere Kund*innen, Partner, staatliche Einrichtungen und Microsoft verursachen, nehmen weiter zu. Das verdeutlicht, wie wichtig ein intensiver Fokus auf Cyberresilienz und eine Zusammenarbeit über alle mit Sicherheit befassten Interessengruppen hinweg ist. Die Gegner greifen auch On-Premises-Systeme an und verschärfen für Unternehmen die Notwendigkeit, Schwachstellen von älteren Systemen durch eine Modernisierung und eine Verlagerung von Infrastruktur in die Cloud, wo die Sicherheit robuster ist, in den Griff zu bekommen.

Wir leben in einer Ära, in der Sicherheit ein wichtiger Faktor für den technologischen Erfolg ist. Innovation und gesteigerte Produktivität lassen sich nur durch die Einführung von Sicherheitsmaßnahmen erreichen, mit denen Unternehmen gegen moderne Angriffe so resilient wie möglich werden. Da digitale Bedrohungen zunehmen und sich weiterentwickeln, ist es von entscheidender Bedeutung, Cyberresilienz in das Gefüge jedes Unternehmens zu integrieren.

Bret Arsenault
Chief Information Security Officer

Cyberresilienz: Eine wichtige Grundlage einer vernetzten Gesellschaft

Im Zuge der Revolution in der digitalen Technologie haben sich Unternehmen transformiert, um ihren Vernetzungsgrad sowohl bei ihrer Betriebsführung als auch in Bezug auf die von ihnen angebotenen Services zu steigern. Da die Bedrohungen in der Cyberlandschaft zunehmen, ist die Integration von Cyberresilienz in die Struktur des Unternehmens ebenso entscheidend wie die finanzielle und betriebliche Resilienz.

Die digitale Transformation hat die Art und Weise, wie Unternehmen mit Kund*innen, Partnern, Mitarbeiter*innen und anderen Beteiligten interagieren, für immer verändert. Neue Technologien bieten riesige Möglichkeiten für die Interaktion mit Menschen, für die Transformation von Produkten und die Optimierung von Abläufen. Die Pandemie hat die digitale Transformation beschleunigt – durch innovative Technologien, mit denen Menschen auf neue Weise und von jedem Standort aus zusammenarbeiten können.

Weil Cyberbedrohungen endemisch werden, gestaltet sich der Schutz vor Kompromittierung für Organisationen in einer stets vernetzten Welt immer schwieriger. Cyberresilienz ist die Fähigkeit eines Unternehmens, trotz einer Flut von Angriffen den Betrieb sowie die Beschleunigung des Wachstums aufrechtzuerhalten. Die Prävention muss gegen die Überlebens- und Wiederherstellungsfähigkeiten abgewogen werden. Staatliche Einrichtungen und Unternehmen entwickeln umfassende Modelle, die über Sicherheit und Datenschutz hinausreichen, um Vermögenswerte, Daten und andere Ressourcen im Rahmen der Cyberresilienz abzusichern.

Entwicklung eines ganzheitlichen Ansatzes für die Cyberresilienz

Cyberresilienz erfordert einen ganzheitlichen, anpassungsfähigen und globalen Ansatz, der den sich entwickelnden Bedrohungen für zentrale Dienste und Infrastruktur standhält, einschließlich:

- Grundlegende Cyberhygiene wie in unserer Glockenkurve zur Cyberresilienz beschrieben.
- Verstehen und Steuern des Kompromisses zwischen Risiken und Vorteilen der digitalen Transformation.
- Funktionen für Reaktionen in Echtzeit, die eine proaktive Erkennung von Bedrohungen und Schwachstellen ermöglichen.
- Schutz vor bekannten Angriffen und präventive Aktivitäten gegen neue und erwartete Angriffsvektoren, einschließlich der Möglichkeit zur automatischen Behebung.
- Verringerung der Auswirkungen von Angriffen und Katastrophen durch Fehlerisolierung und Segmentierung.
- Automatisierte Wiederherstellung und Redundanz im Falle einer Unterbrechung.
- Priorisierung operativer Tests zum Aufspüren von Lücken und Erlangung eines Verständnisses von gemeinsamen Verantwortlichkeiten und Abhängigkeiten von externen Ressourcen, z. B cloudbasierte Sicherheitslösungen.

Ein effektives Programm für Cyberresilienz beginnt mit den Grundlagen in Bezug auf Ressourcen, z. B. das Verstehen der verfügbaren Dienste und die Etablierung eines zuverlässigen Katalogs von Ressourcen, auf die im Falle einer Unterbrechung zurückgegriffen werden kann. Auf dieser Grundlage aufbauend muss das Programm in der Lage sein, seine eigene Effektivität zu bewerten, die Leistung kritischer Dienste und ihre Abhängigkeiten zu messen, Funktionen über On-Premises- und Cloud-Dienste hinweg zu testen und zu validieren sowie kontinuierliche Verbesserungen im gesamten digitalen Lebenszyklus der Organisation zu fördern.

Um einen ganzheitlichen Ansatz zu bieten, arbeiten wir mit Organisationen zusammen, damit sie ihre wichtigsten On-Premises- und Onlinedienste, Geschäftsprozesse, Abhängigkeiten, Mitarbeitenden, Lieferanten und Partner identifizieren können. Wir identifizieren außerdem Vermögenswerte und Ressourcen im Zusammenhang mit Kunden- und Markterwartungen, regulatorischen und vertraglichen Verpflichtungen und internen Prozessen. Während diese wichtigen Ressourcen identifiziert werden, sollten parallele Initiativen für die Erkennung und Überwachung von Bedrohungen, Unterbrechungen, potenziellen Angriffsvektoren sowie von System- und Verfahrensschwachstellen verfolgt werden. Dies trotz des aktuellen Fachkräftemangels zu bewerkstelligen, erfordert eine strenge Priorisierung anhand des Gesamtrisikos für die Organisation.

Diese Art von ganzheitlichem Ansatz muss vor dem Hintergrund einer sich ständig weiterentwickelnden Bedrohungslandschaft anpassungsfähig sein. Das Ziel besteht dabei darin, messbare Leistungssteigerungen zu erzielen, die benötigte Zeit für Erkennung, Reaktion und Wiederherstellung zu senken und den Radius der Auswirkungen im Falle einer Störung zu verkleinern. Der Ansatz muss auch die zunehmenden Verflechtungen von Bedrohungen erkennen. Beispielsweise könnte ein Sicherheitsvorfall zu einer Datenschutzverletzung führen, bei der viele interne und externe Teams zusammenarbeiten müssen, um schnell zu reagieren und die Auswirkungen zu minimieren.

> Cyberresilienz ist die Fähigkeit eines Unternehmens, den Betrieb sowie die Beschleunigung des Wachstums trotz Störungen, einschließlich Cyberattacken, aufrechtzuerhalten.

Umsetzbare Insights

1. Entwickeln und verwalten Sie Technologiesysteme, die die Auswirkungen einer Sicherheitsverletzung einschränken und es Ihnen ermöglichen, selbst bei einem erfolgreichen Eindringversuch sicher und effektiv weiterzuarbeiten. Konzentrieren Sie sich auf typische kritische Ressourcen, unterstützen Sie die Agilität, legen Sie Ihre Architektur auf Anpassbarkeit aus (z. B. hybrid und Multi-Cloud, Multi-Plattform), verringern Sie Angriffsflächen (indem Sie beispielsweise nicht genutzte Anwendungen und zu umfassende Zugriffsrechte entfernen), gehen Sie von kompromittierten Ressourcen aus, und erwarten Sie, dass sich Gegner weiterentwickeln.
2. Berücksichtigen Sie bei der Planung digitaler Projekte neben den Chancen auch potenzielle Bedrohungen, planen Sie auch gemeinsame Verantwortung für die Resilienz in der gesamten digitalen Technologielieferkette ein, einschließlich cloudbasierter Sicherheitslösungen.
3. Entwickeln Sie Systeme, bei denen die Sicherheit schon konstruktionsbedingt integriert ist, und unternehmen Sie Schritte, um zukünftige Bedrohungen zu antizipieren, zu erkennen, ihnen standzuhalten, sich an sie anzupassen und auf sie zu reagieren.
4. Stellen Sie sicher, dass Führungskräfte aus den Fachabteilungen bei Bedarf die Sicherheitsteams konsultieren, um die Risiken im Zusammenhang mit neuen Entwicklungen zu verstehen. Ebenso sollten Sicherheitsteams Geschäftsziele berücksichtigen und Führungskräfte darüber beraten, wie sie diese auf sichere Weise verfolgen können.
5. Stellen Sie sicher, dass für Cybervorfälle eindeutige operative Verfahren und Prozeduren für die Resilienz der Organisation vorhanden sind.

Die Bedeutung der Modernisierung von Systemen und Architekturen

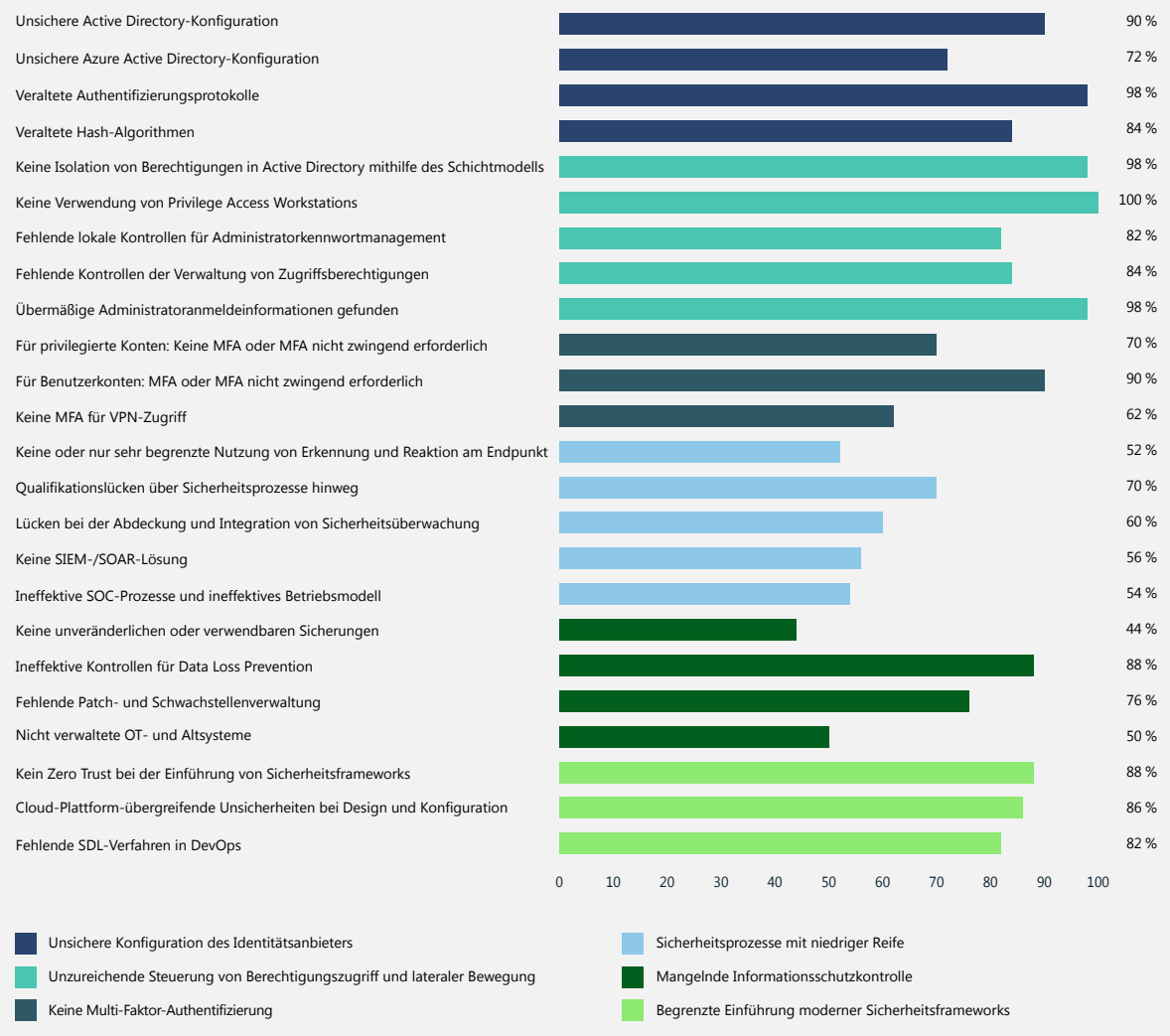
Bei der Entwicklung neuer Funktionen für eine hypervernetzte Welt müssen wir mit Bedrohungen durch ältere Systeme und Software umgehen.

Veraltete Systeme, die vor modernen Konnektivitätstools wie Smartphones, Tablets und Cloud-Diensten entwickelt wurden, sind für Unternehmen, die sie noch einsetzen, ein Risiko. Diese Risikoexposition wird durch die Ergebnisse des Microsoft Security Services for Incident Response-Teams untermauert. Dabei handelt es sich um eine Gruppe von Sicherheitsexpert*innen, die Kund*innen bei der Reaktion auf Angriffe und der Wiederherstellung nach einem Angriff unterstützt.

Im letzten Jahr hingen die Probleme von Kund*innen, die sich von Angriffen erholten, mit sechs Kategorien zusammen, wie das Diagramm auf dieser Seite zeigt. Auf der folgenden Seite werden umsetzbare Schritte hin zu einer verbesserten Resilienz umrissen.

Mehr als 80 % der Sicherheitsvorfälle lassen sich auf einige fehlende Elemente zurückführen, die sich mit modernen Sicherheitsansätzen beheben ließen.

Wichtige Probleme mit Auswirkung auf die Cyberresilienz



Dieses Diagramm zeigt den Prozentsatz der betroffenen Kund*innen, bei denen grundlegende Sicherheitskontrollen fehlen, die für eine Verbesserung der organisatorischen Cyberresilienz entscheidend sind. Die Ergebnisse basieren auf Interaktionen von Microsoft im vergangenen Jahr.

„Führungskräfte sollten Cyberresilienz als eine wichtige Facette von Unternehmensresilienz begreifen. Bei ihren Planungen sollten sie mit Cybervorfällen genauso umgehen, wie sie es mit Naturkatastrophen und anderen unvorhergesehenen Ereignissen tun, und interne Interessengruppen wie Betriebsführung, Kommunikation, Rechtsabteilung und weitere an einem Tisch zusammenbringen, um Strategien zu entwickeln. Dies leistet einen wichtigen Beitrag dazu, dass Organisationen ihre kritischen Geschäftssysteme so schnell wie möglich wieder online bringen können, um zum normalen Geschäftsbetrieb zurückzukehren.

Aber das ist noch nicht alles. Weil sich viele Organisationen auf Dritte wie Lieferanten und Dienstleister verlassen, müssen Führungskräfte deren Wertschöpfungskette von Anfang bis Ende mit einbeziehen, um die Geschäftskontinuität sowie die Unternehmensresilienz weiter zu gewährleisten."

Ann Johnson,
Corporate Vice President of Security, Compliance, Identity, and Management Business Development

Die Bedeutung der Modernisierung von Systemen und Architekturen

Fortsetzung

Es gibt klare Bereiche, um die sich Unternehmen kümmern können, um ihre Herangehensweise zu modernisieren und sich vor Bedrohungen zu schützen:

Problem	Umsetzbare Schritte
Unsichere Konfiguration des Identitätsanbieters Eine fehlerhafte Konfiguration und die Exposition von Identitätsplattformen und ihrer Komponenten sind ein häufiger Vektor für unbefugten Zugriff mit hohen Berechtigungen.	Halten Sie sich beim Bereitstellen und Pflegen von Identitätssystemen wie AD- und Azure AD-Infrastruktur an die Grundlagen und bewährten Methoden für Sicherheitskonfigurationen. Implementieren Sie Zugriffsbeschränkungen, indem Sie für das Verwalten von Identitätssystemen die Trennung von Berechtigungen, Zugriff mit den geringstmöglichen Berechtigungen und PAWs (Privileged Access Workstations) nutzen.
Unzureichende Steuerung von Berechtigungszugriff und lateraler Bewegung Administratoren haben übermäßige Berechtigungen für die gesamte digitale Umgebung und legen auf Workstations, die Internet- und Produktivitätsrisiken ausgesetzt sind, häufig Anmeldeinformationen mit Administratorberechtigung offen.	Schützen und begrenzen Sie den Administratorzugriff, um die Umgebung resilienter zu machen und den Umfang eines Angriffs zu begrenzen. Verwenden Sie Steuerungen für die privilegierte Zugriffsverwaltung wie Just-in-Time-Zugriff und nur die nötigsten administrativen Berechtigungen.
Keine Multi-Faktor-Authentifizierung (MFA) Die Angreifer von heute brechen nicht mehr ein – sie melden sich an.	MFA ist eine lebenswichtige und grundlegende Benutzerzugriffskontrolle, die alle Unternehmen einsetzen sollten. In Kombination mit bedingtem Zugriff kann MFA bei der Bekämpfung von Cyberbedrohungen von unschätzbarem Wert sein.
Sicherheitsprozesse mit niedriger Reife Die meisten betroffenen Organisationen nutzten herkömmliche Tools zur Bedrohungserkennung und besaßen keine relevanten Insights für eine rechtzeitige Reaktion und Behebung.	Eine umfassende Strategie zur Bedrohungserkennung erfordert Investitionen in XDR (Extended Detection and Response) und moderne cloudnative Tools, die Rauschen mithilfe von Machine Learning von Signalen unterscheiden. Modernisieren Sie Tools für die Sicherheitsprozesse, indem Sie XDR integrieren. XDR kann tiefgehende Sicherheits-Insights für die gesamte digitale Landschaft liefern.
Mangelnde Informationsschutzkontrolle Organisationen kämpfen weiterhin damit, ganzheitliche Datenschutzkontrollen zusammenzustellen, die alle Datenspeicherorte abdecken, während des gesamten Informationslebenszyklus wirksam bleiben und sich an der Geschäftsrelevanz der Daten orientieren.	Identifizieren Sie Ihre wichtigen Geschäftsdaten und wo sie sich befinden. Überprüfen Sie die Prozesse des Informationslebenszyklus, und erzwingen Sie Datenschutz, während Sie gleichzeitig die Geschäftskontinuität aufrechterhalten.
Begrenzte Einführung moderner Sicherheitsframeworks Identität ist der neue Sicherheitsperimeter, der den Zugriff auf verschiedene digitale Dienste und Computing-Umgebungen ermöglicht. Durch die Integration von Zero Trust-Prinzipien, Anwendungssicherheit und anderen modernen Cyberframeworks können Organisationen proaktiv mit Risiken umgehen, die sie sich ansonsten kaum vorstellen könnten.	Zero Trust-Frameworks erzwingen Konzepte der geringstmöglichen Berechtigungen, explizite Überprüfung aller Zugriffe und das ständige Antizipieren von Kompromittierungen. Auch in DevOps- und Anwendungslebenszyklusprozessen sollten Organisationen Sicherheitskontrollen und -verfahren implementieren, um höhere Schutzgrade in ihren Geschäftssystemen zu erreichen.

Der grundlegende Sicherheitsstatus ist ein entscheidender Faktor für mehr Lösungseffizienz

Bei unserer Analyse haben wir eine weite Verbreitung von gemeinsamen blinden Flecken in der Verteidigung von Organisationen entdeckt, über die Angreifer einen ersten Zugriff erhalten, einen Brückenkopf einrichten und einen Angriff ausführen können – sogar, wenn moderne Lösungen vorhanden sind.

In vielen Fällen wird das Ergebnis eines Cyberangriffs schon vor dem Beginn des Angriffs an sich festgelegt. Angreifer nutzen vulnerable Umgebungen, um ersten Zugriff zu erhalten, die Umgebung auszuspionieren und über laterale Bewegung sowie Verschlüsselung oder Exfiltrierung Verwüstungen anzurichten. Bei einem frühzeitigen Aufhalten eines Angreifers lässt sich der Gesamtschaden mit größerer Wahrscheinlichkeit geringer halten.

Microsoft hat bestimmte Konfigurationen von Sicherheitsstatus untersucht, um die häufigsten Mängel beim tatsächlichen Betrieb in diesen Umgebungen ausfindig zu machen. Auf diese Weise konnten wir die häufigsten Schwachstellen identifizieren, die bei von Menschen platzierten Ransomware-Angriffen ausgenutzt wurden. Über sie konnten Akteure unerkannt auf ein Netzwerk zugreifen und sich frei in ihm bewegen.

Grundlegende Sicherheitskonfigurationen müssen aktiviert sein

Nicht integrierte oder (sowohl in Bezug auf Schwachstellen als auch in Bezug auf den Status von Sicherheitsagents) veraltete Geräte eines Unternehmens dienen Angreifern als potenzielle Zugänge und Routen zum Etablieren von Zugriff. Wir haben festgestellt, dass es zwar ein wichtiger Schritt ist, Geräte in Organisationen in aktualisierte Lösungen für Erkennung und Reaktion am Endpunkt (EDR)[1] und Endpoint Protection (EPP)[2] einzubinden, doch damit ist noch nicht gewährleistet, dass Ransomware Einhalt geboten wird.

Leistungsstarke Lösungen wie EDR und EPP sind entscheidend, um einen Angreifer frühzeitig in seinem Angriffsfluss zu entdecken und automatisch für Abhilfe und Schutz zu sorgen. Da diese fortschrittlichen Lösungen jedoch auf einer grundlegenden Fähigkeit zum Erkennen eines Angriffs basieren, müssen grundlegende Sicherheitskonfigurationen aktiviert sein. Tatsächlich haben wir eine Häufung von Szenarien beobachtet, in denen die vorhandenen Lösungen durch das Fehlen von grundlegenden Sicherheitskonfigurationen unterminiert wurden.

Bewährte Methoden für die Sicherheitskonfigurationen sind ein besserer Indikator für die Resilienz als die Reaktionszeit von SOC-Analyst*innen (Security Operations Center).

Über einen Zeitraum von sechs Monaten haben wir in unserem gesamten Kunden- und Partnerstamm eine Verkürzung des Zeitbedarfs von einzelnen SOC-Analyst*innen um 70 % beobachtet, um eine relevante Warnung anzuzeigen und darauf zu reagieren. Diese gesteigerte Awareness ist ein gutes Zeichen. Während die Sichtbarkeit der Sicherheitskonfiguration die Leistung der SOC-Analyst*innen verbessert hat, war das Integrieren und Aktualisieren der Geräte in der Organisation ein größerer Einflusswert für eine verbesserte Prävention.

Risiken durch unbekannte Geräte

Im Gegensatz zu Cloud-Netzwerken, bei denen Kund*innen wissen, welche Ressourcen auf welchen Betriebssystemen ausgeführt werden, können On-Premises-Netzwerke eine Vielzahl von Geräten, z. B. IoT, Desktops, Server und Netzwerkgeräte, enthalten, die nicht von der Organisation überwacht oder verwaltet werden.

Das durchschnittliche Unternehmensnetzwerk verfügt über 3.500 vernetzte Geräte, die nicht durch einen EDR-Agent geschützt sind und möglicherweise Zugriff auf Unternehmensressourcen oder sogar auf hochwertige Vermögenswerte haben. Mithilfe der Netzwerküberprüfung entdeckt Microsoft Defender for Endpoint (MDE) Geräte und liefert für die mit dem Netzwerk verbundenen Geräte Informationen über die Geräteklassifikation, z. B. Gerätename, Betriebssystemverteilung und Gerätetyp.

3.500

Durchschnittliche Anzahl von vernetzten Geräten in einem Unternehmen, die nicht durch einen EDR-Agent geschützt sind.

Bei Geräten, die nicht von einem EDR-Agenten unterstützt werden, müssen Sie sich zumindest ihrer Existenz bewusst sein und Maßnahmen zu ihrem Schutz ergreifen. Dazu werten Sie die Schwachstellen aus und schränken den Netzwerkzugriff ein.

Umsetzbare Insights

1. Selbst moderne Lösungen können unterminiert werden, wenn grundlegende Sicherheitskonfigurationen fehlen.
2. Investieren Sie in bewährte Methoden für die Konfigurationen Ihres Sicherheitsstatus, um sich gegen zukünftige Angriffe zu schützen. Diese grundlegenden Einstellungen erzeugen einen massiven Return-on-Investment in Bezug auf die Fähigkeit eines Unternehmens, sich vor Angriffen zu schützen.
3. Integrieren Sie alle relevanten Geräte in eine EDR-Lösung.
4. Achten Sie darauf, Sicherheitsagents zu aktualisieren und den Schutz vor Manipulation sicherzustellen, um die Vorteile einer höheren Transparenz und eines vollständigeren Produktschutzes zu genießen.

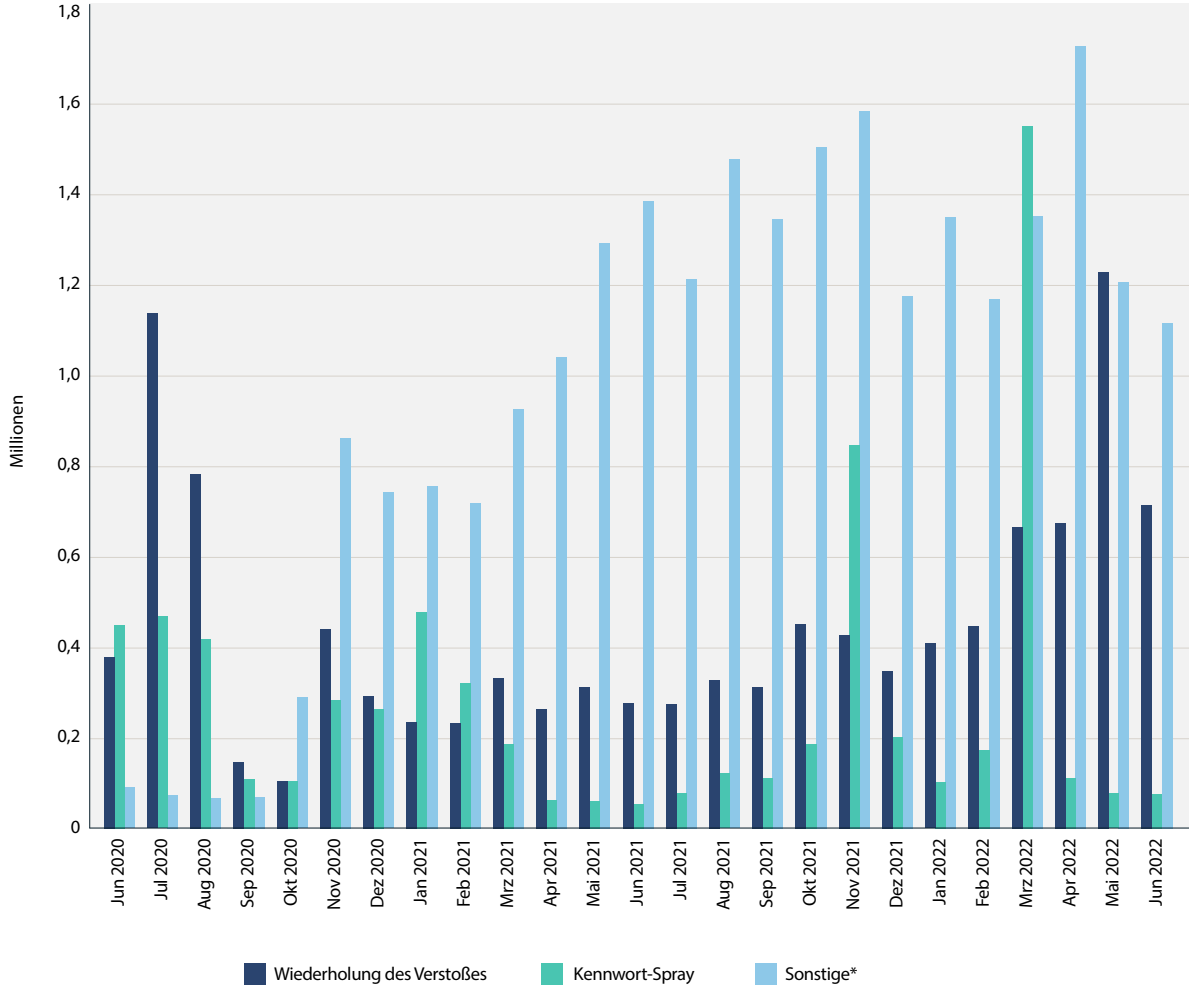
Integre Identitäten sind für den Erfolg von Organisationen von grundlegender Bedeutung

Der Schutz von Identitäten ist wichtiger denn je. Während kennwortbasierte Angriffe die Hauptquelle für die Kompromittierung von Identitäten bleiben, kommen weitere Angriffsarten hinzu. Das Volumen von ausgeklügelten Angriffen steigt gegenüber der früheren Norm bei Kennwort-Spray und „Wiederholung des Verstoßes" weiter an.

Kennwortbasierte Angriffe sind immer noch üblich, und über 90 % der auf diese Weise kompromittierten Konten sind nicht durch eine starke Authentifizierung geschützt. Starke Authentifizierung nutzt mehr als einen Faktor zur Authentifizierung, z. B. Kennwort + SMS und FIDO2-Sicherheitsschlüssel.

Wir haben einen Anstieg bei gezielten Kennwort-Spray-Angriffen beobachtet, wobei sehr große Ausschläge des Angriffsdatenverkehrs über Tausende von IP-Adressen verteilt waren.

Kompromittierte Benutzer*innen nach Angriffskategorie



Kompromittierte Benutzer*innen pro Monat nach Angriffskategorie. Das Volumen von Kennwort-Spray-Angriffen schwankte stark, wie sich anhand der Spitzen im November 2021 und März 2022 zeigt. Diese Spitzen stehen für Tausende von Benutzer*innen und Tausende von betroffenen IP-Adressen. *„Sonstige" bezeichnet Angriffe, die nicht in die Kategorie „Kennwort-Spray" und „Wiederholung des Verstoßes" fielen. Dazu gehörten Phishing, Schadsoftware, Man-in-the-Middle, Kompromittierung von On-Premises-Tokenausstellern und andere. Quelle: Azure AD Identity Protection.

4.500

In der Zeit, die es braucht, um diesen Satz zu lesen, haben wir 4.500 Kennwortangriffe abgewehrt.

Integre Identitäten sind für den Erfolg von Organisationen von grundlegender Bedeutung

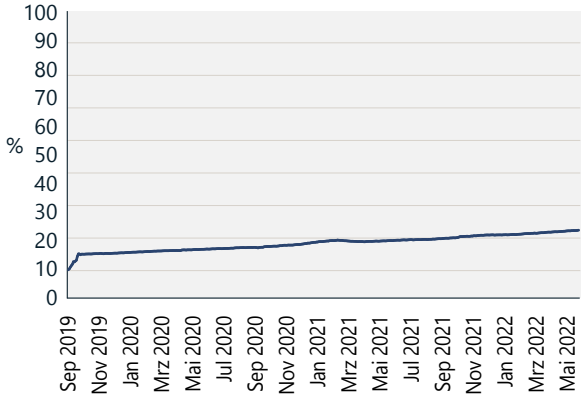
Fortsetzung

Einführung der starken Authentifizierung

Positiv ist, dass wir ein konstantes Wachstum bei der Einführung von starker Authentifizierung in der Unternehmenskundenbasis von Azure Active Directory (Azure AD) feststellen. Bei Azure AD stieg die Anzahl von monatlich aktiven Benutzer*innen (Monthly Active Users, MAU) mit starker Authentifizierung im letzten Jahr von 19 % auf 26 %, während derselbe Parameter bei Administratorkonten von 30 auf zirka 33 % stieg.

Dieser Trend ist positiv, doch nach wie vor bedarf es noch eines erheblichen Wachstums, bis eine Mehrheit mit starker Authentifizierung abgedeckt ist. Kunden, die in ihren Umgebungen noch keine starke Authentifizierung einsetzen, sollten im Sinne des Schutzes ihrer Benutzer*innen mit der Planung und Bereitstellung von starker Authentifizierung beginnen.[3] Beim Entwurf der Bereitstellung von starker Authentifizierung sollte eine kennwortlose Authentifizierung in Betracht gezogen werden, weil sie die sicherste einsetzbare Umgebung bietet und das Risiko von Kennwortangriffen ausschließt.

Nutzung von starker Authentifizierung
(September 2019 – Mai 2022)

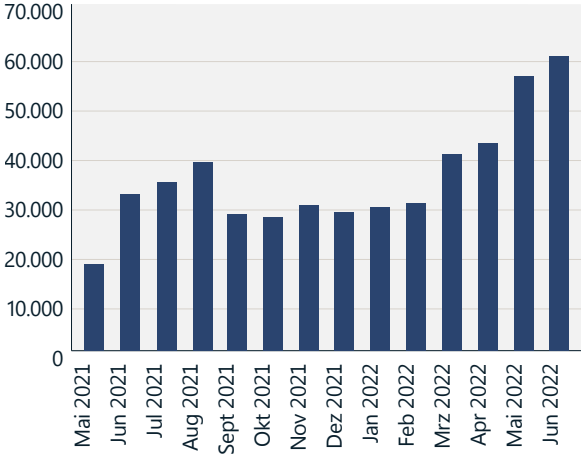


Obwohl sich die Nutzung von starker Authentifizierung seit 2019 verdoppelt hat, verwenden nur 26 % der Benutzer*innen und 33 % der Administrator*innen starke Authentifizierung. Quelle: Azure Active Directory.

Stetige Zunahme von Token Replay-Angriffen

Der Anteil anderer Angriffsformen ist 2022 angestiegen. Wir haben eine Zunahme gezielter Angriffe beobachtet, die insbesondere kennwortbasierte Authentifizierung umgingen, um das Risiko einer Entdeckung zu senken. Diese Angriffe nutzen SSO-Browsercookies (Single Sign-on) oder Aktualisierungstoken, die über Schadsoftware, Phishing und andere Methoden erbeutet worden waren. In einigen Fällen zielten die Angreifer auf Infrastruktur an Standorten in der Nähe des geografischen Standorts der eigentlich vorgesehenen Benutzer*innen, um das Entdeckungsrisiko noch weiter abzuschwächen. Wir haben einen stetigen Anstieg von Token Replay-Angriffen beobachtet, der über 40.000 Erkennungen pro Monat in Azure AD Identity Protection erreichte. Bei „Token Replay“ handelt es sich um die Verwendung von Tokens, die von einem Angreifer, in dessen Besitz sie sind, an legitime Benutzer*innen ausgestellt werden. Token werden häufig über Schadsoftware erbeutet, z. B. durch das Exfiltrieren der Cookies aus dem Browser der jeweiligen Benutzer*innen oder durch fortschrittliche Phishing-Methoden.

Volumen der erkannten Token Replay-Angriffe



Volumen der erkannten Token Replay-Angriffe pro Monat. Quelle: Azure AD Identity Protection, einzelne Sessions wurden durch die Erkennung anomaler Token gekennzeichnet.

Integre Identitäten sind für den Erfolg von Organisationen von grundlegender Bedeutung

Fortsetzung

Extrahieren von Token

Mehr noch als Schadsoftware benötigen Angreifer Anmeldeinformationen, um ihre Ziele zu erreichen. Tatsächlich spielen gestohlene Anmeldeinformationen bei 100 % aller von Menschen platzierter Ransomware-Angriffe eine Rolle. Bei vielen ausgeklügelten Angriffen kommen Anmeldeinformationen zum Einsatz, die aus dem Darknet gekauft wurden und die ursprünglich über recht simple und weit verbreite Schadsoftware zum Stehlen von Anmeldeinformationen erbeutet worden waren. Diese Klasse von Schadsoftware hat sich weiterentwickelt und stiehlt nun auch Token, einschließlich Sessioninformationen und MFA-Anforderungen. Dies bedeutet, dass Infektionen von Homeoffice-Systemen, von denen aus die Benutzer*innen sich bei Unternehmensressourcen anmelden, zu ernsthaften Vorfällen in Unternehmensnetzwerken führen können.

Angreifer können Token auch mithilfe von Man-in-the-Middle-Angriffen von den Geräten der Opfer extrahieren. Bei solchen Angriffen klickt das Opfer auf einen bösartigen Link in einer Phishing-E-Mail oder Sofortnachricht und wird auf eine Website weitergeleitet, die der legitimen Anmeldeseite des Identitätsanbieters zum Verwechseln ähnlich sieht. Tatsächlich handelt es sich dabei um einen Webdienst, der vom Angreifer programmiert wurde und sämtlichen Datenverkehr zwischen den Benutzer*innen und dem Identitätsanbieter abfängt und umleitet. Der Angreifer kann den Benutzernamen und das Kennwort abfischen und auch MFA-Abfragen weiterleiten. Die resultierenden Token, die vom Identitätsanbieter ausgestellt und vom Angreifer abgefangen wurden, enthalten möglicherweise MFA-Ansprüche, die vom Angreifer zum Erfüllen der MFA-Anforderungen verwendet werden können.

Microsoft Defender for Cloud Apps hat seit Anfang 2022 im Durchschnitt 895 solcher Angriffe pro Monat erkannt. Diese Form von Angriffen lässt sich durch die Verwendung von Phishing-resistenten Faktoren verhindern. Dazu gehören beispielsweise zertifikatbasierte Authentifizierung, Windows Hello for Business oder FIDO2-Sicherheitsschlüssel.

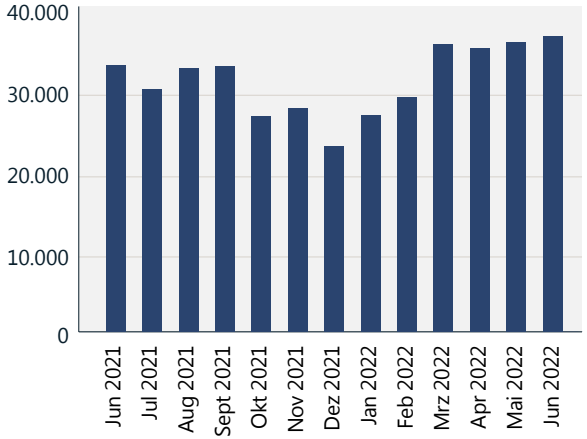
> Kennwortbasierte Angriffe sind die primäre Methode zum Kompromittieren von Konten

MFA Fatigue

Mit dem Konzept der „MFA Fatigue" generieren Angreifer mehrere Anfragen für eine MFA an das Gerät des Opfers. Dabei hegen sie die Hoffnung, dass das Opfer die Anfrage entweder versehentlich oder als Folge von Ermüdung (Fatigue) akzeptiert. Verhindert werden kann dieser Angriff mithilfe moderner Authentifizierungs-Apps wie Microsoft Authenticator in Kombination mit Funktionen wie Zahlenabgleich[4] und der Aktivierung zusätzlichen Kontexts.[5] Nach Schätzungen von Azure AD Identity Protection finden jeden Monat 30.000 MFA Fatigue-Angriffe statt.

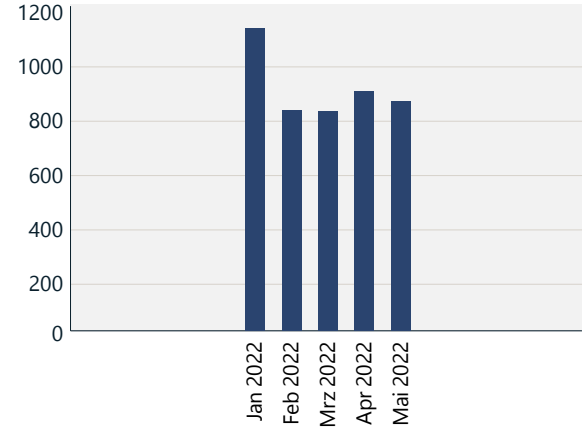
> Der Anteil ausgeklügelter Angriffe steigt weiter, was die Notwendigkeit von Phishing-resistenten Faktoren der Multi-Faktor-Authentifizierung unterstreicht.

Geschätzte Fälle von MFA Fatigue-Angriffen



Quelle: Azure AD Identity Protection.

Erkannte Phishing-Fälle, gefolgt von Man-in-the-Middle-Angriffen.



Quelle: Microsoft Defender for Cloud Apps

Umsetzbare Insights

1. Stellen Sie sicher, dass alle Konten in Ihrer Organisation durch starke Authentifizierung geschützt sind.
2. Kennwortlose Authentifizierung bietet die sicherste und benutzerfreundlichste Umgebung und schließt das Risiko von Kennwortangriffen aus.
3. Deaktivieren Sie veraltete Authentifizierungsmethoden in Ihrer gesamten Organisation.
4. Schützen Sie hochwertige und administrative Konten mit Phishing-resistenten Formen starker Authentifizierung.
5. Wechseln Sie zum Zwecke der Modernisierung von einem On-Premises-Identitätsanbieter zu einem Cloud-Identitätsanbieter, und vernetzen Sie all Ihre Apps mit dem Cloud-Identitätsanbieter, um eine einheitliche User-Experience und Sicherheit zu bieten.

Links zu weiteren Informationen

- This World Password Day consider ditching passwords altogether | Microsoft Security

Standardsicherheitseinstellungen für Betriebssysteme

Angesichts der sich ständig weiterentwickelnden Bedrohungslandschaft erleben wir einen steigenden Bedarf an Computersicherheit, die standardmäßig für ein Verbessern von Cyberresilienz konfiguriert ist. Die Sicherheit des Betriebssystems ist zwar drängender, komplexer und geschäftskritischer als je zuvor, doch die richtige Konfiguration und Verwaltung kann eine Herausforderung sein.

In der Vergangenheit umfasste die Computer- und Gerätesicherheit integrierte Sicherheitsfunktionen, welche die Kund*innen oder IT-Fachleute entsprechend dem jeweils gewünschten Sicherheitsgrad konfigurieren mussten. Dieser Ansatz ist nicht mehr zeitgemäß, weil die Angreifer bei Automatisierung, Cloud-Infrastruktur und Remote-Zugriff inzwischen moderne Tools zum Erreichen ihrer Ziele einsetzen. Es ist heute entscheidend, dass sämtliche Sicherheitsebenen – vom Chip bis zur Cloud – standardmäßig konfiguriert sind. Microsoft konfiguriert die Sicherheit des Windows-Betriebssystems heute standardmäßig vor.[6]

Kunden, die tiefgehende Verteidigungsmaßnahmen implementieren – dazu gehören ein mehrstufiger Sicherheitsstatus, neue Sicherheitsfunktionen, regelmäßiges und konsistentes Patchen und Aktualisieren, aber auch Sicherheitstrainings und Sicherheitsbewusstsein in Bezug auf das Melden von Phishing und anderem Scam –, dürfen mit weniger Schadsoftware rechnen.

Um die Tiefenverteidigung zu vereinfachen, verfügt Windows 11 über einen nahtlos integrierten Hardware- und Softwareschutz, der standardmäßig aktiviert ist, einschließlich Speicherintegrität, Secure Boot und eines Trusted Platform Module 2.0. Mit entsprechend leistungsfähiger Hardware können Windows 10-Benutzer*innen diese Funktionen auch in der App „Windows-Einstellungen" oder im BIOS-Menü aktivieren.

Ältere Geräte haben in der Regel häufig keine so starke Abstimmung zwischen Hardware- und Softwaresicherheitstechniken. Falls möglich, müssen Sie Geräte, bei denen die Sicherheit nicht standardmäßig aktiviert ist, manuell in den Einstellungen konfigurieren.[7]

Für Geräte, bei denen die Sicherheit nicht standardmäßig aktiviert ist, empfiehlt Microsoft, sie möglichst manuell in den Einstellungen zu konfigurieren.

Kümmern Sie sich proaktiv um kontinuierliche Betriebssystemupdates und Sicherheitspatches, die zum Schutz des gesamten Hard- und Softwarelebenszyklus beitragen.

Umsetzbare Insights

1. Verwenden Sie eine kennwortlose Lösung, die Anmeldeinformationen ans Trusted Platform Module bindet. Suchen Sie insbesondere nach einer kennwortlosen Lösung, die dem FIDO-Branchenstandard (Faster Identity Online) entspricht.[8]
2. Führen Sie rechtzeitig eine Bereinigung aller ungenutzten und veralteten ausführbaren Dateien auf den Geräten der Organisation durch.
3. Falls nicht bereits standardmäßig voreingestellt, aktivieren Sie die Speicherintegrität, Secure Boot und Trusted Platform Module 2.0, um fortschrittlichen Firmware-Angriffen vorzubeugen. Dies schützt die integrierten Funktionen in modernen CPUs, die einen Neustart erfordern.
4. Aktivieren Sie die Datenverschlüsselung und den Schutz von Anmeldeinformationen.
5. Aktivieren Sie Anwendungs- und Browsersteuerungen für einen erweiterten Schutz vor nicht vertrauenswürdigen Anwendungen sowie weitere integrierte Schutzmaßnahmen gegen eine Ausnutzung von Schwachstellen.
6. Aktivieren Sie Schutz für Speicherzugriff, um sich vor eventuellen physischen Angriffen zu schützen, beispielsweise, wenn jemand ein verseuchtes Gerät mit einem von extern zugreifbaren Port verbindet.

Links zu weiteren Informationen

- Windows Security Book | Commercial
- New security features for Windows 11 will help protect hybrid work | Microsoft Security Blog

Zentralität der Softwarelieferkette

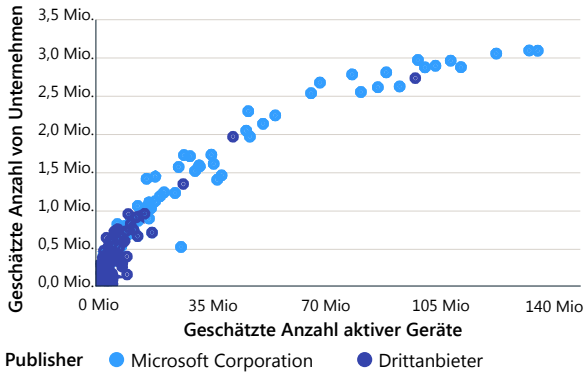
Angriffe auf Apps, Plugins und Erweiterungen von Drittanbietern können das Kundenvertrauen in Lieferanten untergraben, die in der Versorgungsinfrastruktur allerdings eine zentrale Rolle spielen. Das Zurateziehen von Netzwerktheorie beim Betrachten von Softwarezentralität hilft dabei zu verstehen, wie wichtig Patchen gerade für zentrale Apps ist.

Das Windows-App-Netzwerk mit 18 Millionen ausführbaren Anwendungen ist bei fünf Millionen Organisationen installiert und in Nutzung und bietet einen Top-Level-Überblick über unsere Softwareinfrastruktur. Von den 100.000 am häufigsten verwendeten Anwendungen stammen 97 % von Drittanbietern, die ihre Updates und Sicherheitspatches auch selbst verwalten. Dies zeigt zwei wichtige Merkmale unserer kommerziellen Anwendungsinfrastruktur auf.

Erstens gibt es Zentralität in der Windows-Infrastruktur für kommerzielle Anwendungen. Nur die beliebtesten 100.000 (von 18 Millionen) Anwendungen werden auf 1.000 oder mehr Geräten verwendet. Mit anderen Worten: Nur knapp über die Hälfte von einem Prozent dieser Anwendungen hat eine derart weitrechende Wirkung in der Geräteinfrastruktur.

Zweitens gibt es Vielfalt bei der Verwaltbarkeit solcher Anwendungen, wobei die Anbieter der beliebtesten 10.000 Anwendungen die Updates und Sicherheitspatches dieser am häufigsten verwendeten kommerziellen Anwendungen verwalten. Dies zeigt die Interdependenz eines Unternehmens mit einer Vielzahl von Sicherheits-, Compliance- und Verwaltungskontrollen von Softwareanbietern.

Kommerzielle Durchdringung der am häufigsten genutzten Anwendungen



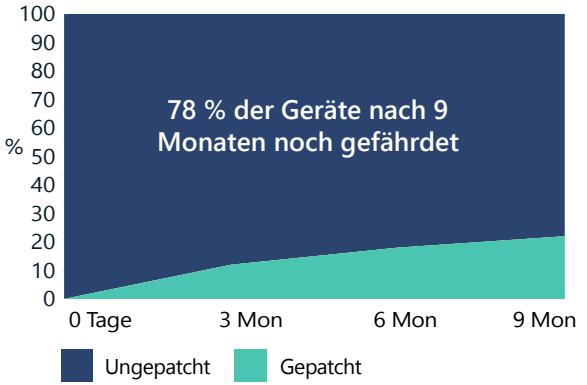
Die wichtigsten Anwendungen werden von Millionen von Organisationen und zig Millionen von Geräten verwendet. Weil sie praktisch überall vorhanden sind, suchen Cyberkriminelle ständig nach ausnutzbaren Schwachstellen in diesen beliebtesten Anwendungen. Und diese können Millionen von Geräten in der Benutzerbasis betreffen.

Wir beobachten Millionen von kommerziellen Geräten, die noch viele Monate nach der Veröffentlichung von Patches – oder sogar Jahre nach Auslaufen des Produktsupports – verwundbare Anwendungsversionen verwenden. Zum Beispiel gibt es mehr als eine Million aktive kommerzielle Windows-Geräte, auf denen eine PDF Reader-Version ausgeführt wird, die seit 2017 nicht mehr unterstützt wird.

Auf Millionen von kommerziellen Geräten bleiben alte und nicht mehr unterstützte Versionen von Anwendungen in der aktiven Nutzung. Daher laufen solche Organisationen Gefahr, Schwachstellen zu haben, die nicht mehr gepatcht werden.

Bei Anwendungsversionen, für die noch Support besteht, beobachten wir ein Plateau bei der Einführungsgeschwindigkeit kritischer Patches. Das ist das Gegenteil eines Trends zu mehr Resilienz. Zum Erreichen der erforderlichen Resilienz sollte die Kurve bei der Einführung von Patches Monat für Monat eine exponentielle Steigung aufweisen.

Bereitstellungsquote von kritischen Patches



Nach der Untersuchung einer kritischen Schwachstelle, die 134 Versionen einer Reihe von Browsern betraf, haben wir festgestellt, dass 78 % – das sind Millionen von Geräten – auch neun Monate nach der Veröffentlichung des Patches noch eine der betroffenen Versionen verwendeten.

Mit dem InterpretML[9]-Toolkit haben wir Eigenschaften identifiziert, die mit den Organisationen korrelieren, die vermutlich Geräte mit älteren App-Versionen haben. Zu den wichtigsten Einflusswerten gehörten dabei: geringe Stundenzahl für die Nutzung auf den Geräten, geografische Bereiche wie Asien-Pazifik und Lateinamerika und Branchen wie Automobilindustrie, Chemie, Telekommunikation, Transport und Logistik, Gesundheitskostenträger (Anspruchsregulierer) und Versicherungen.

Zur Aufrechterhaltung von Softwareresilienz sollte es auch gehören, nicht genutzte Anwendungen regelmäßig zu deaktivieren oder zu deinstallieren.

Die Sicherheit und die Compliance einer Organisation hängen von den eigenen Bemühungen und von den Bemühungen ihrer Softwarelieferanten ab.

Umsetzbare Insights

1. Führen Sie in Ihrer gesamten Organisation rechtzeitig Updates aller Anwendungen und Endpunkte durch.
2. Führen Sie rechtzeitig eine Bereinigung aller ungenutzten und veralteten ausführbaren Dateien auf den Geräten der Organisation durch.

Links zu weiteren Informationen

- Microsoft Intune documentation | Microsoft Docs
- Manage apps | Microsoft Docs
- Microsoft Defender for Endpoint | Microsoft Security
- OSS Secure Supply Chain Framework | Microsoft Security Engineering
- Microsoft Open Source Software Secure Supply Chain Framework | GitHub

Entwickeln von Resilienz gegenüber neuen DDoS-, Webanwendungs- und Netzwerkangriffen

Die beschleunigte digitale Transformation hat das herkömmliche Modell von Netzwerken und Sicherheitsperimetern beendet. Der Umstieg auf die Cloud bedeutet, dass Unternehmen für den Schutz digitaler Ressourcen die cloudnative Netzwerksicherheit nutzen müssen.

Komplexität, Häufigkeit und Menge der Angriffe nehmen weiter zu und sind nicht mehr auf saisonale Ereignisse begrenzt. Vielmehr verzeichnen wir eine Entwicklung hin zu ganzjährigen Angriffen. Dies unterstreicht die Bedeutung eines kontinuierlichen Schutzes, der über die herkömmlichen Spitzenzeiten im Datenverkehr hinausgeht.

Distributed-Denial-of-Service-Angriffe (DDoS)

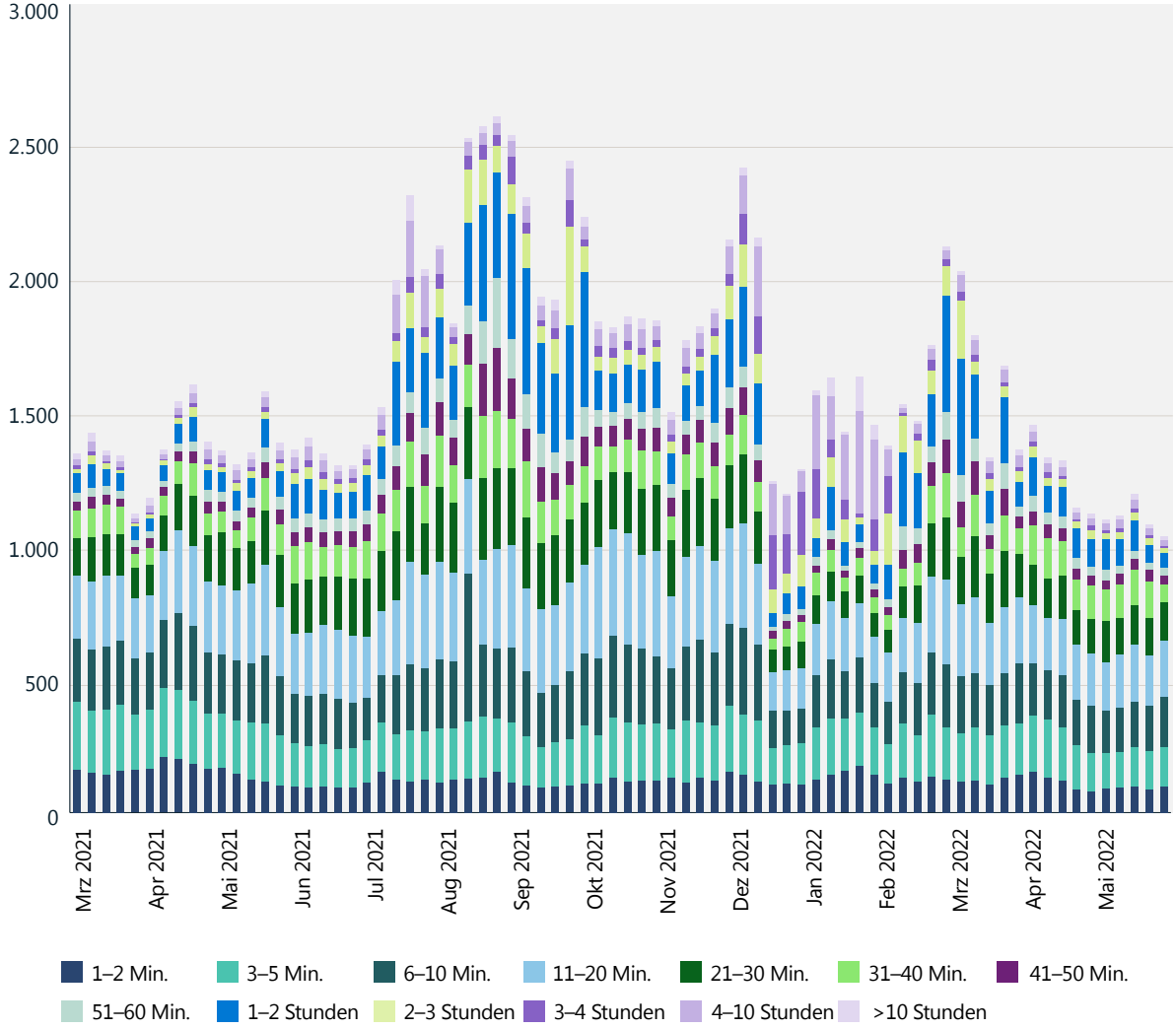
Im letzten Jahr erlebte die Welt eine DDoS-Aktivität, die in Bezug auf Volumen, Komplexität und Häufigkeit beispiellos war. Hinter dieser Explosion von DDoS-Angriffen steckte ein erheblicher Anstieg von nationalstaatlichen Angriffen und eine kontinuierliche Verbreitung von kostengünstigen DDoS-for-Hire-Services. Microsoft hat durchschnittlich 1.955 Angriffe pro Tag entschärft, eine 40-prozentige Steigerung gegenüber dem Vorjahr. Früher trat die höchste Zahl der Angriffe normalerweise während der Feiertage am Jahresende auf. In diesem Jahr wurden die meisten Angriffe jedoch am 10. August 2021 verzeichnet. Dies könnte darauf hindeuten, dass sich die Angriffe nun über das ganze Jahr verteilen, und es macht deutlich, wie wichtig fortlaufender Schutz auch außerhalb der herkömmlichen Spitzenzeiten ist.

Im November 2021 vereitelte Microsoft einen volumetrischen DDoS-Angriff mit einem Durchsatz von 3,4 Terabit pro Sekunde (Tbps), der aus etwa 10.000 Quellen aus mehreren Ländern stammte. Ähnliche hochvolumetrische Angriffe von mehr als 2 Tbps wurden auch 2022 entschärft. Dies verdeutlicht, dass nicht nur die Komplexität und Häufigkeit der Angriffe zunehmen, sondern auch ihr Volumen (Bandbreite).

Angriffsdauer

Die meisten Angriffe, die im letzten Jahr beobachtet wurden, waren von kurzer Dauer. Etwa 28 % der Angriffe dauerten weniger als zehn Minuten, 26 % dauerten zehn bis 30 Minuten und 14 % dauerten 31 bis 60 Minuten. Bei 32 % der Angriffe betrug die Dauer mehr als eine Stunde.

Anzahl von DDoS-Angriffen und Verteilung der Dauer
(März 2021 – Mai 2022)



Die meisten Angriffe im letzten Jahr waren von kurzer Dauer. Etwa 28 % der Angriffe dauerten weniger als zehn Minuten.

Entwickeln von Resilienz gegenüber neuen DDoS-, Webanwendungs- und Netzwerkangriffen

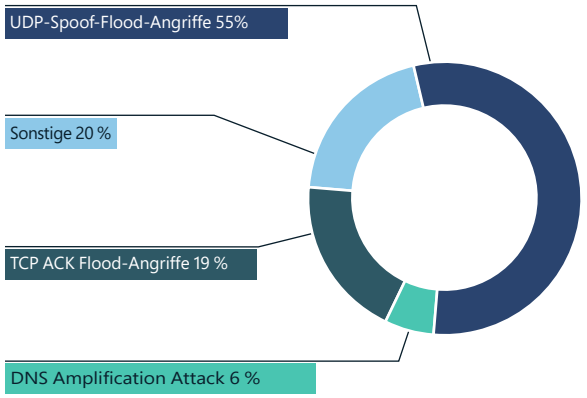
Fortsetzung

DDoS-Angriffsvektoren

Die am häufigsten verwendeten Angriffsvektoren des letzten Jahres waren UDP (User Datagram Protocol), Spiegelung auf Port 80 mithilfe von SSDP (Simple Service Discovery Protocol), CLDAP (Connectionless Lightweight Directory Access Protocol), DNS (Domain Name System) und NTP (Network Time Protocol), die für eine einzelne Spitze verantwortlich waren. Wir haben auch eine Zunahme von DDoS-Angriffen auf Websites feststellen können, mit einem Spitzenwert von 16,3 Millionen RPS (Requests per Second) und 9,89 Tbps Datenverkehr.

2022 hat Microsoft täglich fast 2.000 DDoS-Angriffe entschärft und den größten jemals gemeldeten DDoS-Angriff vereitelt.

DDoS-Angriffsvektoren



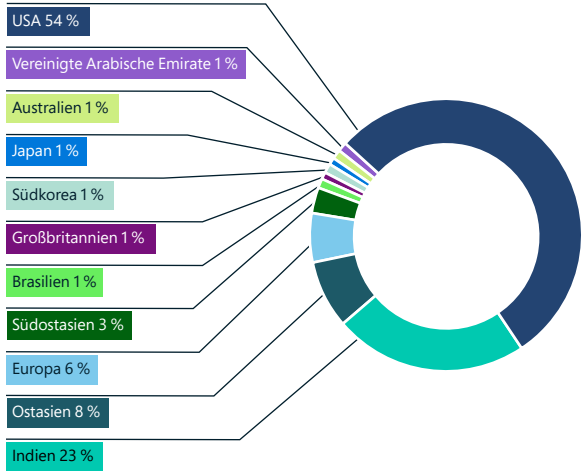
Mit einem Anstieg von 16 auf 55 % wurden UDP-Spoof-Flood-Angriffe in der ersten Jahreshälfte 2022 zum häufigsten Vektor. TCP-ACK-Flood-Angriffe gingen dagegen von 54 auf 19 % zurück.

Die Gaming-Branche ist nach wie vor das häufigste Ziel von DDoS-Angriffen. Diese erfolgen meistens mit Mutationen des Mirai-Botnets und niedervolumigen UDP-Protokollangriffen. Aufgrund der häufigen Verwendung von UDP in Gaming- und Streaminganwendungen bestand eine überwältigende Mehrheit der Angriffsvektoren aus UDP-Spoof-Floods. UDP-Spiegelungen und Verstärkungsangriffe machten hingegen nur einen kleinen Anteil aus.

Geografische Zielregionen

Von den im letzten Jahr festgestellten DDoS-Angriffen erfolgten 54 % gegen Ziele in den USA. Dieser Trend lässt sich möglicherweise teilweise durch den Umstand erklären, dass die meisten der Azure- und Microsoft-Kund*innen in den USA angesiedelt sind. Wir haben auch einen starken Aufwärtstrend bei Angriffen gegen Indien gesehen – von nur 2 % aller Angriffe in der zweiten Jahreshälfte 2021 auf 23 % in der ersten Jahreshälfte 2022. Ostasien, insbesondere Hongkong, bleibt mit 8 % ein beliebtes Ziel. In Europa konzentrierten sich die Angriffe auf Regionen wie Amsterdam, Wien, Paris und Frankfurt.

Ziele von DDoS-Angriffen

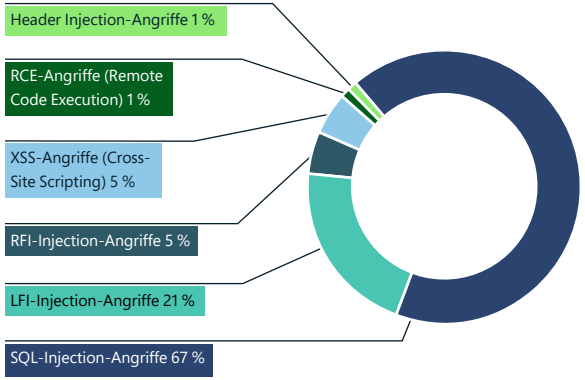


Wir führen die hohe Anzahl von Angriffen in Asien auf die riesige Stellung zurück, die Gaming in dieser Region einnimmt, vor allem in China, Japan, Südkorea und Indien. Diese Bedeutung wird eher noch zunehmen, da die wachsende Präsenz von Smartphones die Beliebtheit von mobilem Gaming weiter befeuert. Das legt nahe, dass dieses geografische Ziel künftig noch verstärkt in den Fokus rücken wird.

Ausnutzung von Webanwendungen

In Kombination mit DDoS-Schutz macht WAF (Web Application Firewall) einen integralen Bestandteil einer Strategie der Tiefenverteidigung für den Schutz von Web- und API-Ressourcen (Application Programming Interface) aus. Microsoft hat jeden Monat mehr als 300 Milliarden über Azure WAFs ausgelöste WAF-Regeln beobachtet.

Verteilung der häufigsten Angriffstypen



Azure WAF erkennt täglich Milliarden von Angriffen, die zu den OWASP Top 10[10] (Open Web Application Security Project) gehören. Laut unseren Signalen bestanden die Angriffsversuche zumeist aus SQL-Injection-Angriffen, gefolgt von lokalen und remote durchgeführten File-Injection-Angriffen. Dies entspricht der Liste der OWASP Top 10. Dort werden Injection-Angriffe als die dritthäufigste Art von Webangriffen aufgeführt.

Es gab auch einen Anstieg von Bot-Angriffen auf Azure-Webanwendungen: Jeden Monat fanden durchschnittlich 1,7 Milliarden Bot-Anfragen statt, und 4,6 % dieses Datenverkehrs bestanden aus bösartigen Bots.

Entwickeln von Resilienz gegenüber neuen DDoS-, Webanwendungs- und Netzwerkangriffen

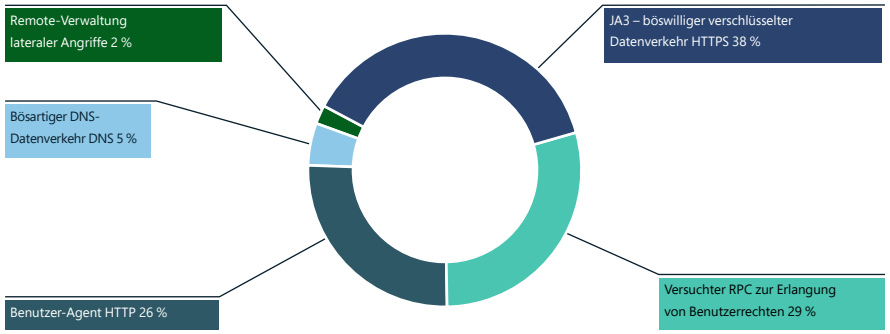
Fortsetzung

Aufgrund der zunehmenden Anzahl von Bots, die Angriffe zum Stehlen von Anmeldeinformationen, zum Kreditkartenbetrug, für Kampagnen zur Einflussnahme im Cyberspace oder für Attacken auf Lieferketten durchführten, erwarten wir einen stetigen Anstieg von Bot-Angriffen auf Webanwendungen.

Erkennung und Abwehr von Angriffen auf Netzwerke

Wir haben 2022 eine deutliche Zunahme von Exploits auf Netzwerkebene beobachtet, vor allem in Form von Schadsoftware. Das IDPS (Intrusion Detection and Prevention System) von Azure Firewall blockierte mehr als 150 Millionen Verbindungen alleine im Monat Juni.

Gründe für die IDPS-Verweigerung von Datenverkehr



Gründe für IDPS-Warnungen über Datenverkehr

Die Analyse von IDPS-Warnungen und -Verweigerungen von Datenverkehr zeigt die folgenden Herangehensweisen der Angreifer: Bei der Verweigerung von Datenverkehr sehen wir, dass Angreifer SSL zum Verbergen ihrer Aktivitäten einsetzen, und die Remote-Ausführung von Angriffen nimmt an Häufigkeit zu. Bei den Warnungen über Datenverkehr sehen wir, dass SMB-/SMB2-Protokolle für die Remote-Ausführung von Angriffen zum Einsatz kommen.

Umsetzbare Insights

1. Überprüfen Sie den gesamten Datenverkehr zwischen den Systemen in einem Rechenzentrum oder Cloud-Dienst sowie den Datenverkehr, der auf sie zugreifen will.
2. Entwickeln Sie eine robuste ganzjährige Strategie für die Netzwerksicherheit.
3. Nutzen Sie cloudnative Sicherheitsdienste, um einen robusten Zero Trust-Sicherheitsstatus für das Netzwerk zu implementieren.

Links zu weiteren Informationen

- Improve your security defenses for ransomware attacks with Azure Firewall | Azure Blog and Updates | Microsoft Azure
- Anatomy of a DDoS amplification attack | Microsoft Security Blog
- Intelligent application protection from edge to cloud with Azure Web Application Firewall | Azure Blog and Updates | Microsoft Azure

Entwicklung eines ausgewogenen Ansatzes für Datensicherheit und Cyberrsesilienz

Die digitale Transformation hat eine enorme Ausweitung der Datenressourcen sowie einen Anstieg bei den Risiken für Sicherheit, Compliance und Datenschutz befeuert. Cyberresiliente Organisationen müssen Investitionen in Datenschutz-, Compliance- und Wiederherstellungsfunktionen gegeneinander abwägen und sie mit spezialisierten regulatorischen Reaktionsverfahren zur Behebung verschiedener Arten von Verstößen bündeln.

Bei Datenschutzverletzungen geht es nicht darum, ob sie stattfinden, sondern wann. Die Studie „Cost of a Data Breach, 2021" von IBM und dem Ponemon Institute schätzt die Kosten von Datenschutzverletzungen weltweit auf durchschnittlich 4,24 Millionen USD (ein Anstieg von 10 % gegenüber dem Vorjahr); für die USA liegt dieser Wert bei 9,05 Millionen USD. Zu den größten kostentreibenden Faktoren zählten Compliance-Verstöße. Umgekehrt wurden Kostensenkungen bei Verstößen bewährten Methoden wie IR-Planung (Incidence Response), Reifegrad der Zero Trust-Bereitstellung, Einsatz von KI und Automatisierung für die Sicherheit und Verschlüsselung zugeschrieben.

Datenschutzverletzungen sind unvermeidlich. Organisationen, die bei der Resilienz einen ausgewogenen Ansatz verfolgen, werden die Häufigkeit, die Auswirkungen und die Kosten von Verstößen senken.

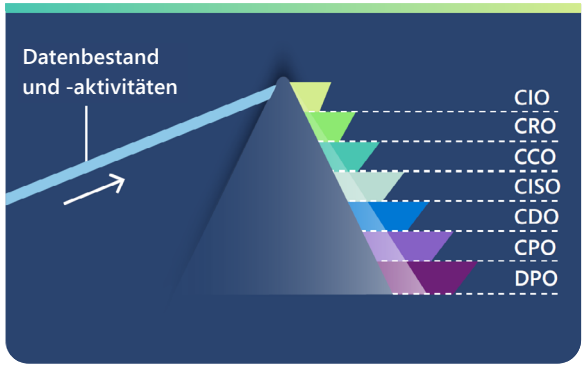
Data Governance, Sicherheit, Compliance und Datenschutz hängen zusammen

Wir haben erlebt, wie Daten in den letzten Jahren als Wertschöpfungsfaktor für Organisationen immer mehr an Bedeutung gewonnen haben. Gleichzeitig weichen neue Datenschutzregulierungen, die sowohl Data Governance als auch Sicherheit verlangen, die früheren Grenzen zwischen den Rollen der Risikoverantwortlichen auf. Während neuere Rollen auf C-Level, z. B. CDO (Chief Data Officer) oder CPO (Chief Privacy Officer), ein großes Interesse an Sicherheit und Compliance haben, setzt die Implementierung und Umsetzung von Datenschutz häufig auf Teams, die vom CIO (Chief Information Officer) und/oder CISO (Chief Information Security Officer) geleitet werden. Es handelt sich dabei nicht um eine Einbahnstraße, weil die von CDOs geleiteten Initiativen zur Data Governance ebenfalls Sicherheitsvorteile mit sich bringen. Aufgrund dieser Verzahnung müssen IT-, Data Governance-, Sicherheits-, Compliance- und Datenschutzteams noch enger zusammenarbeiten, um die Effizienz zu steigern und Risiken zu steuern.

Einheitliche Plattformen für das Risikomanagement des gesamten Datenbestands einer Organisation sind die Zukunft

Die Abstimmung der Verwaltungsprozesse für IT, Data Governance, Sicherheit, Compliance und Datenschutz gestaltet sich in einer Umgebung mit hochgradig angepassten Anwendungen für jeden dieser Bereiche schwierig. Auch die nicht einheitliche Abdeckung in der üblicherweise hybriden und über mehrere Clouds verteilten Datenstruktur einer Organisation erschwert die Kontrolle. Unserer Auffassung nach benötigen Organisationen eine zentrale Konsole, damit sie ihren gesamten Datenbestand ermitteln und identifizieren, ihre Daten schützen, den Zugriff, die Nutzung und den Lebenszyklus steuern sowie Datenverlust verhindern können.

Das Arbeiten mit demselben Datenbestand und denselben Aktivitätsinformationen erleichtert teamübergreifende Prozesse, liefert einen umfassenderen Risikoüberblick und ermöglicht Organisationen, sich besser auf eine Datenschutzverletzung vorzubereiten und ihre Reaktion darauf zu optimieren.



Diese zentrale Konsole fungiert dabei als eine Art Prisma. Teams, die für Datensicherheit, Compliance und Datenschutz zuständig sind, benötigen unterschiedliche, aber dennoch einheitliche Ansichten desselben Datenbestands und derselben Datenaktivität, um sich aufeinander abzustimmen und zusammenzuarbeiten. Zu Datenaktivitäten zählen der Zugriff auf sowie die Bearbeitung und Verlagerung von Daten, und sie alle sind wertvolle Elemente in der Datensicherheitsgleichung.

Data Governance, Sicherheit, Compliance und Datenschutz sind voneinander abhängig und erfordern teamübergreifende Zusammenarbeit, um effektiv zu sein.

Umsetzbare Insights

1. Wägen Sie Verteidigung und Wiederherstellung gegeneinander ab, und minimieren Sie die Auswirkungen von Datenschutzverletzungen, indem Sie in Compliance, Datenschutz und Reaktionsfähigkeit investieren.
2. Entwickeln und nutzen Sie Prozesse und Tools, die siloartige Datenrisiken verringern und stattdessen den gesamten Datenbestand abdecken.

Links zu weiteren Informationen

- Microsoft Purview – Data Protection Solutions | Microsoft Security
- The future of compliance and data governance is here: Introducing Microsoft Purview | Microsoft Security Blog

Resilienz gegenüber Operationen zur Einflussnahme im Cyberspace: Die menschliche Dimension

In den letzten fünf Jahren haben Fortschritte in den Bereichen Grafik und Machine Learning benutzungsfreundliche Tools hervorgebracht, die eine schnelle Erstellung hochwertiger, realistischer Inhalte ermöglichen, die sich innerhalb von Sekunden über das ganze Internet verbreiten können.

Bei Ereignissen, die in Form von Text-, Audio- und Videoinhalten gemeldet werden, haben wir einen Punkt erreicht, an dem weder Menschen noch Algorithmen Fakten zuverlässig von Fiktion unterscheiden können. Die Verbreitung dieser Tools und der mit ihnen erzeugten Produkte werfen Zweifel an der Glaubwürdigkeit sämtlicher digitaler Medien auf und führen zu Verwerfungen bei unserem Verständnis lokaler und weltweiter Ereignisse. Neue Formen von Beeinflussungsoperationen, die durch technologische Fortschritte möglich wurden, haben gravierende Auswirkungen auf demokratische Prozesse.[11]

Es stellt sich die Frage, was wir tun können, um Vorbereitungen für eine resilientere Zukunft gegenüber einer derartigen Einflussnahme im Cyberspace zu treffen. Technologie ist jedoch nur ein Baustein. Es wird vieler Anstrengungen bedürfen, einschließlich der Förderung von Medienkompetenz, Sensibilisierung und Wachsamkeit, Investitionen in Qualitätsjournalismus – mit vertrauenswürdigen Reportern vor Ort und auf lokaler, nationaler und internationaler Ebene –, Netzwerken für die Meldung von und Warnung vor Beeinflussungsoperationen sowie neuer Arten von Regulierung, die böswillige Akteure sanktionieren, wenn sie digitale Medien mit der Absicht einer Täuschung erzeugen oder manipulieren.

Uns ist bewusst, dass die Wiederherstellung von Vertrauen in digitale Inhalte ein ehrgeiziges Ziel ist, das vielfältige Sichtweisen und Beteiligungen erfordert. Es gibt nicht das eine Unternehmen, die eine Institution oder die eine Regierung, das oder die diese Bedrohungen im Alleingang bewältigen könnte. Doch durch die Zusammenarbeit vieler lässt sich Großes bewirken. Das ist besonders wichtig, weil jetzt alle – Regierungen, Branchen, der akademische Sektor und vor allem Medienunternehmen auf der ganzen Welt – für eine bessere und gesunde Gesellschaft zusammenarbeiten müssen.

Links zu weiteren Informationen

- Applications for artificial intelligence in Department of Defense cyber missions | Microsoft On the Issues
- Artificial Intelligence and Cybersecurity: Rising Challenges and Promising Directions. Anhörung über die Anwendungen künstlicher Intelligenz für den Einsatz im Cyberspace vor dem Unterausschuss für Cybersicherheit des Senatsausschusses für die Streitkräfte, 117. Kongress (3. Mai 2022; Aussage von Eric Horvitz)

Stärkung des Faktors Mensch durch Weiterbildung

Die Berücksichtigung des Faktors Mensch ist ein wichtiger Bestandteil jeder Cybersecurity-Schulungsstrategie. Laut der Kapersky-Studie „Human Factor in IT Security“[12] spielen bei 46 % der Cybervorfälle unvorsichtige oder schlecht informierte Mitarbeiter*innen eine Rolle, die den Angriff unabsichtlich ermöglichen.

Das Education and Awareness-Team von Microsoft in der Organisation für Digital Security and Resilience ist verantwortlich, beim Thema Cybersicherheit den Faktor Mensch zu stärken und Mitarbeiter*innen zu befähigen, ihre eigenen Systeme und Daten sowie die unserer Kund*innen zu schützen. Unsere Ziele sind folgende:

- Reduzierung des Risikos für Microsoft und unsere Kund*innen durch den Aufbau zentralisierter unternehmensweiter Kernkompetenzen im Bereich Cybersicherheit bei allen Mitarbeitenden
- Stärkung der Sicherheitskompetenz der Mitarbeiter*innen durch einen mehrstufigen Ansatz zur Vertiefung von Trainings, um gewünschte Verhaltensweisen zu fördern
- Förderung einer Kultur des Wandels, indem Sicherheitsbewusstsein zum integralen Bestandteil der Kultur von Microsoft erhoben wird, verstärkt durch jährliche verpflichtende Sicherheitstrainings und -events
- Bereitstellung einer zentralen Webressource mit bewährten Methoden, Informationen zu Unternehmensrichtlinien und Meldungen von sämtlichen Vorfällen im Zusammenhang mit Cybersicherheit

Für alle Microsoft-Mitarbeiter*innen wird mindestens einmal jährlich ein gezieltes, zentralisiertes Qualifizierungsprogramm angeboten. Die Trainingsangebote sind darauf optimiert, aktuelle Initiativen für Cybersicherheit zu unterstützen und messbare Verhaltensergebnisse zu liefern. Das Information Risk Management Council (IRMC) von Microsoft spielt eine wichtige Rolle beim Identifizieren wichtiger Ergebnisse von Verhaltensänderungen in Bezug auf Cybersicherheit, die durch die Trainings erreicht werden sollen.

Wo immer möglich, messen wir bei all unseren Qualifizierungsprogrammen zur Cybersicherheit die Effizienz, die Effektivität sowie die Ergebnisse der Lösung. Beispielsweise erreicht unser Angebot von Trainings zu Insiderbedrohungen eine Erfolgsrate von 95 %, mit außerordentlichen Zufriedenheitswerte bei den Lernenden. Zudem hat es zu einem deutlichen Anstieg bei den von Führungskräften eingereichten Meldungen von Fällen von Insiderbedrohungen geführt, die über das unternehmenseigene Tool „Report It Now“ erfolgen. Das Programm umfasst:

Security Foundations: Zentralisiertes, unternehmensweites Training zu Awareness und Compliance beim Thema Cybersicherheit, die sich mit wesentlichen Sicherheits- und Datenschutzpraktiken befasst. Diese hochkarätige Serie von Trainings setzt auf ein Edutainment-Modell, um das Lernen über Cybersicherheit spannend und interessant zu gestalten.

STRIKE: Das obligatorische technische Training von Microsoft für Ingenieur*innen, die Fachbereichslösungen entwickeln und pflegen.

Die Teilnahme an diesem Training ist nur auf Einladung möglich. Es befasst sich mit zeitkritischen und zentralen Bereichen der bewährten Methoden für Cybersicherheitshygiene und wird über ein hybrides Präsenzmodell angeboten, das auf den Bedarf der Zielgruppe zugeschnitten ist.

Programmspezifisch: Gezielte Trainingsprogramme unterstützen spezifische Initiativen zur Cybersicherheit, z. B. Schatten-IT, Insiderbedrohungen und Microsoft Federal. Diese Angebote sind eng mit der übergeordneten Beteiligungsstrategie ihrer jeweiligen Cybersicherheitsinitiativen verzahnt. Dies wird gewährleistet über eine Unterstützung seitens der Unternehmensleitung sowie durch Feedback in Form von Scorecards, um einen Ansatz, bei dem nur Kästchen angekreuzt werden, zu verhindern.

MSProtect: Die zentrale Webressource von Microsoft bietet bewährte Methoden, Informationen zu Unternehmensrichtlinien und Meldungen von Vorfällen für alles, was mit Cybersicherheit zusammenhängt. Diese On-Demand-Ressource eignet sich für Mitarbeiter*innen außerhalb von formellen Trainingsangeboten.

Sicherheitsschulungen sollten nicht als lästige Pflicht gesehen werden, bei der nur Kästchen angekreuzt werden. Konzentrieren Sie sich stattdessen auf Verhaltensänderungen, die überprüfbare Resultate bei den vereinbarten gewünschten Verhaltensweisen ermöglichen, und etablieren Sie Prüfsysteme, um die Wirkung der Angebote zu bewerten.

Umsetzbare Insights

1. Bieten Sie Ihren Mitarbeiter*innen Sicherheitstrainings an, wann und wo immer sie nötig sind.
2. Entwickeln Sie eine zentralisierte Qualifizierungsstrategie, in die Kenntnisse von sämtlichen Interessengruppen aus dem gesamten Unternehmen einfließen.
3. Sorgen Sie dafür, dass die Wirkung des Trainings nachverfolgt wird sowie Effizienz (Quantity), Effektivität (Qualität) und Ergebnisse (geschäftliche Auswirkungen) analysiert werden.

Links zu weiteren Informationen

- Microsoft startet die nächste Phase seiner Qualifizierungsinitiative, nachdem es schon 30 Millionen Menschen geholfen hat

Insights aus unserem Programm zur Eliminierung von Ransomware

Microsoft verfolgt für die eigene Cybersicherheit seit fünf Jahren konsequent den Zero Trust-Ansatz[13], um sicherzustellen, dass Identitäten und Geräte robust verwaltet werden und in einwandfreiem Zustand sind. Weil das Risiko durch Ransomware wächst, haben wir eine umfassende Perspektive entwickelt, um unseren Schutzansatz für uns selbst und für unsere Kund*innen zu unterstützen.

Nach einer eingehenden internen Evaluierung haben wir ein Programm zur Eliminierung von Ransomware entwickelt, um Lücken bei Kontrollen und Abdeckungen zu schließen, einen Beitrag zu Funktionsverbesserungen bei Diensten wie Defender for Endpoint, Azure und Microsoft 365 zu leisten sowie um Playbooks für unsere SOC- und Engineering-Teams zu erstellen, damit sie wissen, wie sie im Falle eines Ransomware-Angriffs eine Wiederherstellung durchführen.

Der erste Schritt bestand darin, ein Verständnis unseres Schutzes vor einem gegen Microsoft gerichteten Ransomware-Angriff zu erlangen. Maßnahmen zur Bereitstellung von Defender for Endpoint und zur Sicherstellung, dass alle Geräte verwaltet werden und unseren Zero Trust-Richtlinien entsprechen, waren bereits in vollem Gange. Wir mussten aber dennoch eine Möglichkeit finden, sämtliche Facetten der größeren Fragestellung zu verstehen: Würden wir uns effektiv von einem Angriff erholen können? Um dem auf den Grund zu gehen, haben wir unsere bekannte Liste von Kontrollen mit NIST 8374: Ransomware Risk Management: A Cybersecurity Framework (CSF) Profile[14] abgeglichen. Dieses Dokument entspricht im Wesentlichen unseren allgemeinen Unternehmensrichtlinien. Bei dieser Analyse traten schnell Lücken in der Abdeckung zutage.

Als Nächstes haben wir Lücken in den CSF-Funktionen zum Identifizieren, Erkennen, Schützen, Reagieren und Wiederherstellen priorisiert. Wir haben eine strategische Ausrichtung auf Zero Trust und andere Programme gefunden und außerdem Lücken entdeckt, für die es keine Arbeitsabläufe gab. Nach einer Schätzung des Aufwands zum Beheben dieser Lücken haben wir sie in zwei Kategorien eingeteilt:

- **Schutz des Unternehmens (Protect the Enterprise, PtE):** Definieren von Arbeitsaufgaben, die wir als Unternehmen durchführen müssen, um uns zu schützen und uns schnell von einem erfolgreichen Angriff erholen zu können.
- **Schutz der Kund*innen (Protect the customer, PtC):** Integrieren von Funktionen in unsere Angebote, die unsere Kund*innen wie auch unser Business schützen.

Integrieren der Befunde in unser eigenes Unternehmen

Um die größten Risiken zu entschärfen und unsere kritischen Dienste vor einem Ransomware-Angriff zu schützen, werden wir unsere Investitionen in den nächsten sechs bis zwölf Monaten auf die fünf nachfolgenden Szenarien konzentrieren. Dies erfolgt als Teil eines dedizierten Ransomware-Programms. Sobald wir in jedem einzelnen dieser Szenarien erfolgreich sind, werden wir den Umfang des Programms allmählich auf alle Teile des Unternehmens ausdehnen.

Szenario 1: Die Mitglieder des Sicherheitsteams verstehen das Gesamtrisiko im Zusammenhang mit einem Ransomware-Angriff und haben ein Verfahren etabliert, um die Unternehmensführung über Kontrolllücken und den Risikostatus zu informieren.

Szenario 2: Die Mitglieder des Sicherheitsteams haben Zugriff auf Playbooks, die darauf ausgelegt sind, ihnen und anderen Teams innerhalb von Microsoft bei der Reaktion auf einen Ransomware-Angriff sowie bei der Wiederherstellung kritischer Dienste nach so einem Angriff zu helfen.

Szenario 3: Die Mitglieder des Enterprise Resilience-Teams verfügen über einen Standard, dem sie beim Sichern kritischer Systeme folgen können. Es gibt Playbooks und es erfolgen regelmäßig Sicherungs- und Wiederherstellungsübungen, um sicherzustellen, dass die Daten im Falle eines Ransomware-Angriffs wiederhergestellt werden können.

Szenario 4: Service-Verantwortliche verstehen und implementieren die erforderlichen Sicherheits- und Betriebskontrollen sowie Richtlinien für den Schutz ihrer Dienste, ihrer Kundendaten, Endpunkte und Netzwerkressourcen vor Ransomware-Angriffen. Besonderer Fokus liegt dabei auf Services, die als kritische Dienste für Microsoft priorisiert sind.

Szenario 5: Alle Mitarbeiter*innen haben Zugang zu Fortbildungs- und Trainingsressourcen, in denen beschrieben wird, wie sich ein Ransomware-Angriff erkennen lässt und auf welche Weise das Sicherheitsteam zu informieren und die Reaktion anzustoßen ist.

Umsetzbare Insights

1. Dokumentieren und validieren Sie durchgängige Wiederherstellungs- und Sanierungsaktivitäten im Zusammenhang mit Ransomware-Angriffen auf kritische Dienste.
2. Beziehen Sie Interessengruppen bei der Aktualisierung Ihrer Playbooks zum Krisenmanagement Ihres Unternehmens mit ein, um darin auf Ransomware bezogene Aktivitäten mit aufzunehmen sowie einen Entscheidungsfindungsprozess und eine Anleitung zur Bestimmung, ob/wann ein Lösegeld gezahlt werden sollte.
3. Verbessern Sie die Erkennung und die Schutzabdeckung, indem Sie Funktionen in Ihren bereitgestellten Sicherheitsprodukten aktivieren (z. B. Regeln zum Reduzieren der Angriffsfläche in Defender for Endpoint).
4. Arbeiten Sie mit dem für Sicherheitsstandards zuständigen Team an der Definition einer Baseline für den Schutz vor einem Ransomware-Angriff, und stellen Sie Ihren Technikerteams Training und Dokumentation zur Vorgehensweise beim Schutz vor einem Ransomware-Angriff zur Verfügung.
5. Nutzen Sie Automatisierung, um die Bereitstellung von Sicherheits- und Betriebsrichtlinien für die DevOps-Teams zu erleichtern und um eine schnelle Meldung und Behebung zu gewährleisten, wenn ein System aus der Compliance fällt.

Links zu weiteren Informationen

- Sharing how Microsoft protects against ransomware | Microsoft Inside Track

Handeln Sie in Bezug auf die Auswirkungen von Quantensicherheit

Der größte Druck liegt darin, mit der Bedrohung für die heutige Kryptografie und für alles, was sie beschützt, umzugehen. Das kürzlich veröffentlichte Memorandum on Improving the Cybersecurity of National Security Department of Defense and Intelligence Community Systems[15] baut auf der US Executive Order 10428[16] for Improving the Nation's Cybersecurity auf und betont, dass die Sicherheit der Softwarelieferkette für den Umgang mit zukünftigen nationalstaatlichen Angriffen von entscheidender Bedeutung ist.

Was sind Quantencomputer?

Quantencomputer sind Computer, die sich die Eigenschaften der Quantenphysik zunutze machen, um Daten zu speichern und Berechnungen durchzuführen. Bei bestimmten Aufgaben kann dies extrem nützlich sein. Dort schlagen sie selbst unsere besten Supercomputer um Längen. Quantencomputer eröffnen schon jetzt ganz neue Möglichkeiten bei der Verschlüsselung und Verarbeitung von Daten. Studien prognostizieren, dass Quantencomputer bereits 2030 ein milliardenschwerer Industriezweig sein werden.[17] Tatsächlich stehen Quantencomputer und Quantenkommunikation bereit, um eine transformative Wirkung über eine Vielzahl von Branchen hinweg zu entfalten – vom Gesundheitswesen und dem Energiesektor bis hin zu Finanzdienstleistungen und Sicherheit.

Quantencomputer sind eine Bedrohung für die heutige Kryptografie und alles, was sie beschützt.

Die Bedrohung für die heutige Kryptografie

Mit dem Shor-Algorithmus aus dem Jahr 1994 und einem industriellen Quantencomputer von mehr als einigen Millionen physischen Qubits könnten alle unsere derzeit weit verbreiteten kryptografischen Algorithmen für öffentliche Schlüssel wirksam gebrochen werden. Es ist von entscheidender Bedeutung, über „quantensichere" Kryptosysteme nachzudenken, sie auszuloten und sie zu standardisieren. Solche Systeme müssen effizient, flexibel und vor jedem gegnerischen quantenbasierten Angriff geschützt sein. Die Migration von Software hin zu einer „Postquantenkryptografie", d. h. vorhandene klassische Algorithmen und Protokolle, die vor Quantenangriffen geschützt sind, wird Jahre dauern – wenn nicht sogar mindestens ein Jahrzehnt.[18]

Das bedeutet, dass der größte Druck darin liegt, mit der Bedrohung für die heutige Kryptografie und für alles, was sie beschützt, umzugehen. Angreifer können verschlüsselte Daten heute aufzeichnen und sie später ausnutzen, sobald ein Quantencomputer verfügbar ist. Wenn wir erst auf Quantencomputer warten, bevor wir uns um die kryptografischen Auswirkungen kümmern, wird es zu spät sein.

Weil Kryptografie in der gesamten Cyberinfrastruktur eingesetzt wird, könnten unsere auf Kryptografie basierenden Sicherheitsdienste kompromittiert werden. Dazu gehören beispielsweise Dienste für die Kommunikation (TLS, IPsec), Messaging (E-Mail, Webkonferenzen), Identitäts- und Zugriffsverwaltung, Web-Browsing, Code-Signing, Zahlungstransaktionen und andere Dienste, deren Schutz von Kryptografie abhängig ist.

Wenn Quantencomputer Realität werden, müssen auch Softwarekomponenten von Drittanbietern, in denen kryptografische Algorithmen und Funktionen implementiert sind, besser überwacht werden. Dazu müssen alle Unternehmen entlang der Wertschöpfungskette ihren Beitrag leisten, damit eine fortgesetzte Sicherheit der Kette gewährleistet ist. Branchengremien und staatliche Einrichtungen verstärken ihre Anstrengungen darin, Sicherheitsauflagen für die Softwarelieferkette zu definieren und, in einigen Fällen, neue Mandate für die Absicherung der Kette einzuführen. Das National Security Memorandum NSM-8[19] legt Anforderungen und Zeiträume für das Implementieren von Postquantenkryprografie (Post-Quantum Cryptography, PQC) in nationalen Sicherheitssystemen (NSS) fest. Es sieht einen Zeitrahmen von 180 Tagen vor für die „Modernisierungsplanung, Verwendung von nicht unterstützter Verschlüsselung, genehmigte missionsspezifische Protokolle und Planung für den Einsatz quantenresistenter Kryptografie, wo erforderlich".

Beim Übergang hin zu einer quantensicheren Kryptografie ist Standardisierung eine Aktivität mit langer Vorlaufzeit. Normungsgremien, die an Standards für die Kryptografie öffentlicher Schlüssel arbeiten, müssen heute damit anfangen, mit Postquantenalgorithmen zu experimentieren und sich entsprechend anzupassen.

Neue Algorithmen für die Postquantenkryptografie (PQC) – klassische Algorithmen, die als robust gegen Quantenangriffe gelten – werden derzeit vom Post-Quantum-Standardization Project des NIST geprüft.[20] Diese Arbeit wird sich auch auf die weltweiten Initiativen innerhalb der Normungsgremien auswirken. Auch wenn es einige Überschneidungen mit der Algorithmusauswahl der US-Regierung geben mag, können abweichende Entscheidungen nationaler Gremien in Bezug auf konforme Algorithmen zu internationalen Herausforderungen führen. Diese Fragmentierung wird wiederum die Entwicklung von Produkten und Diensten erschweren.

Neue Algorithmen für die Postquantenkryptografie werden derzeit vom Post-Quantum Cryptography Standardization-Programm des NIST geprüft. Diese Arbeit wird sich auch auf die weltweiten Initiativen innerhalb der Normungsgremien auswirken.

Umsetzbare Insights

Zusammen mit SAFECode und Partnermitgliedern sollten von der Branche sofortige, kurzfristige Initiativen zur Vorbereitung auf den Übergang zu PQC vorgenommen werden.[21] Dazu gehören:

1. Bestandsaufnahme Ihrer Produkte/Codes, die Kryptografie verwenden
2. Implementieren einer Strategie für Kryptoagilität in Ihrer gesamten Organisation. Dazu gehört die Minimierung des erforderlichen Code-Churns, wenn sich die Kryptografie ändert.
3. Pilotprojekte für die Nutzung quantensicherer Algorithmen in Ihren Produkten oder Diensten, in denen Kryptografie eingesetzt wird
4. Bereitschaft zur Verwendung verschiedener Algorithmen für Verschlüsselung, Schlüsselaustausch und Signaturen bei öffentlichen Schlüsseln
5. Testen Ihrer Anwendungen in Bezug auf die Auswirkungen sehr großer Schlüsselgrößen, Chiffren und Signaturen

Links zu weiteren Informationen

- Microsoft has demonstrated the underlying physics required to create a new kind of qubit | Microsoft Research

Integration von Business-, Sicherheits- und IT-Anforderungen für mehr Resilienz

Robuste Cyberresilienz hängt davon ab, wie Führungskräfte beim Implementieren von Sicherheit mit Sicherheitsteams zusammenarbeiten. Nach der Erfahrung von Microsoft ist Sicherheitsführerschaft eine herausfordernde Disziplin, die Unterstützung von Vordenkern in der Organisation erfordert, um das Unternehmen möglichst effektiv zu schützen.

Security-Verantwortliche bewegen sich in einem breiten Spektrum dynamischer Herausforderungen. Dabei reichen die Themen von Risiko, Technologie, Wirtschaft, organisatorischen Abläufen und Geschäftsmodellen bis hin zu kultureller Transformation, geopolitischen Interessen, Spionage und der Einhaltung internationaler Sanktionen. Jeder dieser Punkte birgt Nuancen, die verstanden werden müssen und auf die genau eingegangen werden muss.

Sicherheitsexpert*innen haben außerdem die Aufgabe, intelligente, gut finanzierte und hoch motivierte menschliche Angreifer genauso abzuwehren wie schlecht qualifizierte, aber effektive Internetkriminelle. Ihre Teams müssen komplexe technische Infrastrukturen verteidigen, die häufig über mehr als 30 Jahre allmählich aufgebaut wurden. Und damals genoss Sicherheit nur eine geringe oder überhaupt keine Priorität. Entscheidungen, die vor Jahren getroffen wurden, können heute Risiken darstellen, bis wir die technischen Schulden bezahlen und die Sicherheitslücken beseitigen.

Business-Entscheider und Richtlinienverantwortliche können einen erheblichen positiven Einfluss auf die Sicherheit haben, indem sie die Sicherheitsexpert*innen aktiv unterstützen und dabei helfen, eine Brücke zwischen integrierter Sicherheit und dem Rest des Unternehmens zu schlagen. Wenn Microsoft mit Kunden zusammenarbeitet, die auf diese Weise aufgestellt sind, erleben wir, wie sie eine resilientere Organisation aufbauen und außerdem ihre Agilität für Anpassungen und Innovationen verbessern.

Mitglieder der Führungsetage können Sicherheitsexpert*innen unterstützen, indem sie sich auf drei Schlüsselbereiche konzentrieren:

1. Security by Design

Sicherheit wird manchmal als Hindernis oder nachträglicher Aspekt in Geschäftsprozessen betrachtet, der häufig nur dann bei Entscheidungen Berücksichtigung findet, wenn es zu spät ist, um ein Risiko zu vermeiden oder es leicht und kostengünstig zu beheben.

Business-Entscheider und Richtlinienverantwortliche müssen sicherstellen, dass sie:

Sicherheit frühzeitig in neuen Initiativen integrieren. Neue digitale Initiativen und die Einführung der Cloud sollten die Sicherheit an erste Stelle setzen, um zu gewährleisten, dass das Risiko für die Organisation nicht mit jeder neuen Anwendung oder digitalen Funktion größer wird. Sobald die Sicherheit zuverlässig integriert ist, können Sie solche Prozesse zum Modernisieren von Altsystemen verwenden. Auf diese Weise schöpfen Sie gleichzeitig Sicherheits- und Produktivitätsvorteile ab.

Präventive Wartung beim Thema Sicherheit zum Standard erheben. Vergewissern Sie sich, dass grundlegende Sicherheitswartung – wie die Anwendung von Sicherheitsupdates und Patches sowie von sicheren Konfigurationen – vollständige Unterstützung der Organisation genießt (einschließlich Budgets, geplanter Ausfallzeiten, Beschaffungsanforderungen in Bezug auf den anbieterseitigen Produktsupport).

Leider verzögern oder verschieben viele Unternehmen diese gängigen Praktiken oder wenden sie nur teilweise an. Dies öffnet Angreifern Tür und Tor. Die Notwendigkeit für eine Normalisierung von Sicherheit wird in US NIST 800-40 abgebildet.[22]

2. Befassung mit Sicherheit

Business-Entscheider sollten sich aktiv an Sicherheitsprozessen beteiligen und sie fördern, um die angemessene Priorisierung von Ressourcen und eine gute Vorbereitung auf eventuelle Sicherheitskatastrophen zu gewährleisten. Dazu gehört die Mitwirkung bei Folgendem:

Identifizierung wichtiger Geschäftsressourcen. Sicherheitsexpert*innen und -teams müssen wissen, welche Komponenten unternehmenskritisch sind, damit sie die Sicherheitsressourcen auf das Wesentliche konzentrieren können. Dies ist oft eine neue Aufgabe, die das Stellen und Beantworten neuer Fragen beinhaltet, um die sich zuvor nie jemand gekümmert hat.

Cybersicherheitsübungen für Geschäftskontinuität und Notfallwiederherstellung. Cyberangriffe können zu großen Ereignissen werden, die den gesamten Geschäftsbetrieb stören oder komplett lahmlegen. Wenn jedoch die Teams in der ganzen Organisation auf den Umgang mit solchen Situationen vorbereitet sind, verkürzt dies die Zeit bis zur Wiederaufnahme des Geschäftsbetriebs, begrenzt den Schaden für die Organisation und trägt dazu bei, das Vertrauen von Kund*innen, Bürger*innen und anderen Anspruchsgruppen aufrechtzuerhalten. Dies sollte in einen vorhandenen Prozess zur Geschäftskontinuität und Notfallwiederherstellung integriert sein.

Entscheidungen über Sicherheitsrisiken werden am besten von jenen Verantwortlichen getroffen, die einen vollständigen Überblick über alle Risiken und Chancen haben.

Integration von Business-, Sicherheits- und IT-Anforderungen für mehr Resilienz

Fortsetzung

3. Die richtige Sicherheitspositionierung

Die Art und Weise, wie Unternehmen die Verantwortung für Sicherheitsrisiken strukturieren, entscheidet darüber, ob sie gute oder schlechte Risikoentscheidungen treffen. Risikoentscheidungen werden am besten von jenen Verantwortlichen getroffen, die einen vollständigen Überblick über alle Risiken und Chancen haben, aber Organisationen weisen die entsprechende Zuständigkeit häufig (implizit oder explizit) Fachexpert*innen im Sicherheitsteam zu. Dies ist eine ungesunde Belastung für Sicherheitsteams und nimmt Unternehmer*innen die Transparenz und Kontrolle über ein zentrales Risiko für ihr Unternehmen. Organisationen können dies auf folgende Weise korrigieren:

Vorbereitung von Unternehmer*innen: Geben Sie der Geschäftsleitung einen Gesamtüberblick, und unterrichten Sie sie darüber, wie sich Bedrohungen auf ihr Unternehmen auswirken können und werden. Die direkte Einbindung von Sicherheitsteams in diese Initiativen stärkt auch die kollegiale Zusammenarbeit und die geschäftliche Agilität insgesamt.

Zuweisung von Sicherheitsrisiken zu Unternehmer*innen: Wenn Unternehmer*innen genug Informationen erhalten, um das Sicherheitsrisiko zu verstehen und zu akzeptieren, sollte die Organisation die Verantwortlichkeit für Sicherheitsrisiken ausdrücklich auf sie übertragen, wobei die Verantwortung für die Verwaltung dieses Risikos und dafür, dass die Unternehmer*innen mit Fachwissen und Handlungsempfehlungen versorgt werden, bei den Sicherheitsteams bleibt.

„Cyberresilienz ist eine gleitende Skala: von klassischer Geschäftskontinuität und Notfallwiederherstellung, die bei guter Datensicherung beginnt, über Wiederherstellungsfunktionen für Prozesse, Technologie und ihre Abhängigkeiten (einschließlich Personen und Dritte) bis hin zu dauerhaft aktiven Selbstheilungsdiensten, Resilienz für kritische Rollen und Failover für kritische Drittanbieter. Die resilientesten Organisationen fördern die Integration zwischen IT, Geschäftsleiter*innen und Sicherheitsexpert*innen. Zuverlässige Resilienz muss von Anfang an Bestandteil des Designs sein und ein sicheres Change Management sowie granulare Fehlerisolation umfassen. Cyberresilienz ist nur ein Szenario in einem guten Programm, das alle Gefahren einplant. Weil die Cyberrisiken zunehmen und die Schnittstelle zwischen Cybersicherheit und Resilienz immer wichtiger wird, ergibt sich auch eine engere Verknüpfung zwischen dem CISO (Chief Information Security Officer) und dem Resilienzprogramm eines Unternehmens. Jedes Jahr übernehmen mehr CISOs die Verantwortung für die unternehmensweite Resilienz."

Lisa Reshaur
General Manager, Risk Management, Microsoft

Links zu weiteren Informationen

- From resilience to digital perseverance: How organizations are using digital technology to turn the corner in unprecedented times | Official Microsoft Blog
- How IT and security teams can work together to improve endpoint security | Microsoft Security

Die Glockenkurve zu Cyberresilienz

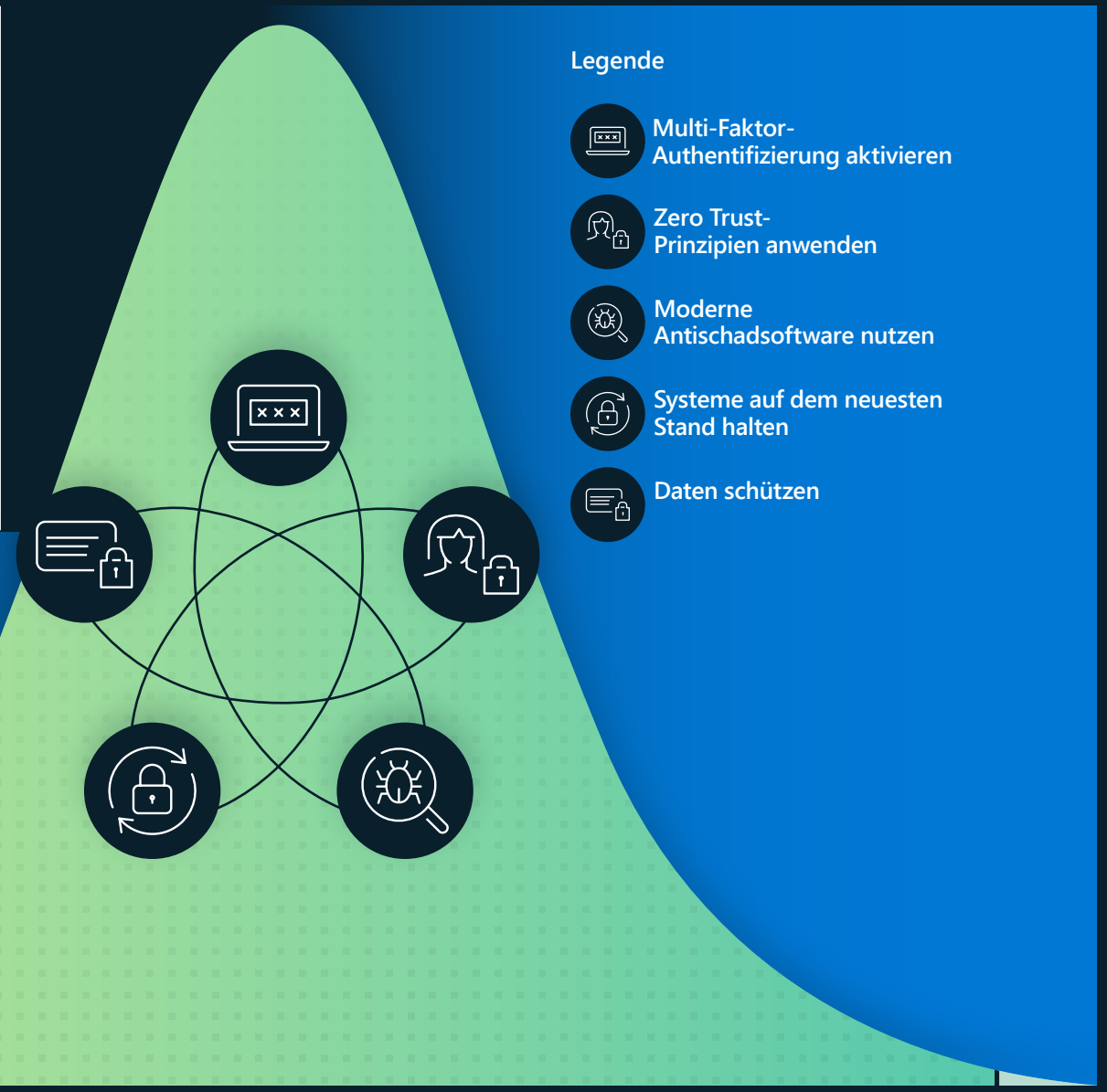
Erfolgsfaktoren für Resilienz, die jedes Unternehmen einführen sollte

Wie wir gesehen haben, sind viele Cyberangriffe einfach deshalb erfolgreich, weil die grundlegende Cyberhygiene nicht eingehalten wurde. Jede Organisation sollte folgende Mindeststandards einführen:

- **Aktivieren der Multi-Faktor-Authentifizierung (MFA):** Zum Schutz vor kompromittierten Benutzerkennwörtern und für zusätzliche Resilienz für Identitäten.
- **Anwenden von Zero Trust-Prinzipien:** Der Eckpfeiler jedes Resilienzplans, der die Auswirkungen für eine Organisation begrenzt. Diese Prinzipien sind:
  - Explizite Prüfung: Vergewissern Sie sich, dass sich Benutzer*innen und Geräte in einem guten Zustand befinden, bevor Sie den Zugriff auf Ressourcen zulassen.
  - Zugriff mit den geringstmöglichen Berechtigungen: Lassen Sie nur die Berechtigung zu, die für den Zugang zu genau einer Ressource benötigt wird und zu keiner weiteren.
  - Assume Breach: Gehen Sie davon aus, dass die Systemverteidigung verletzt wurde und möglicherweise Systeme kompromittiert sind. Dies bedeutet, dass die Umgebung ständig auf mögliche Angriffe überwacht werden muss.
- **Nutzung von umfassender Antischadsoftware für Erkennung und Reaktion:** Implementieren Sie Software zum Erkennen und automatischen Blockieren von Angriffen, die auch Insights für die Sicherheitsprozesse bereitstellt. Das Überwachen von Insights aus Bedrohungserkennungssystemen ist unverzichtbar für die rechtzeitige Reaktion auf Bedrohungen.
- **Aktualität:** Ungepatchte und veraltete Systeme sind eine zentrale Ursache dafür, dass viele Organisationen einem Angriff zum Opfer fallen. Stellen Sie sicher, dass alle Systeme aktuell sind, einschließlich Firmware, Betriebssystem und Anwendungen.
- **Schutz für Daten:** Die Kenntnis Ihrer wichtigen Daten, deren Speicherorte und ob die richtigen Systeme implementiert sind, ist entscheidend für die Implementierung des geeigneten Schutzes.

98 %

Grundlegende Sicherheitsmaßnahmen schützen immer noch vor 98 % der Angriffe.



Fußnoten

1. Erkennung und Reaktion am Endpunkt (Endpoint Detection and Response, EDR) ist eine Endpunkt-Sicherheitsplattform, die Unternehmen dabei unterstützt, komplexe Bedrohungen in ihren Netzwerken zu verhindern, zu erkennen, zu untersuchen und darauf zu reagieren. Die EDR-Funktionen ermöglichen die Erkennung fortgeschrittener Angriffe nahezu in Echtzeit. Sicherheitsanalyst*innen können Warnungen effektiv priorisieren, Transparenz in Bezug auf den Umfang von Verstößen gewinnen und korrigierende Maßnahmen ausführen, um Bedrohungen zu beseitigen.
2. Eine Endpoint Protection Platform (EPP) ist eine Lösung, die auf Endpunktgeräten bereitgestellt wird, um dateibasierte Schadsoftware zu unterbinden, bösartige Aktivitäten von vertrauenswürdigen und nicht vertrauenswürdigen Anwendungen zu entdecken und zu blockieren und die Ermittlungs- und Sanierungsfunktionen bereitzustellen, die für eine dynamische Reaktion auf Sicherheitsvorfälle und Warnungen erforderlich sind.
3. https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted
4. https://docs.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-number-match
5. https://docs.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-additional-context
6. Windows Security Book: Commercial
7. New security features for Windows 11 will help protect hybrid work | Microsoft Security Blog
8. FIDO Alliance: Open Authentication Standards More Secure than Passwords
9. https://interpret.ml/
10. OWASP Top Ten | OWASP Foundation
11. https://blogs.microsoft.com/on-the-issues/2022/05/03/artificial-intelligence-department-of-defense-cyber-missions/
12. https://www.kaspersky.com/blog/the-human-factor-in-it-security/
13. https://aka.ms/ZTatMSFT
14. https://csrc.nist.gov/publications/detail/nistir/8374/final
15. https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/
16. Executive Order 14028 Improving the Nation's Cybersecurity
17. https://thequantumdaily.com/2020/02/18/the-quantum-computing-market-size-superpositioned-for-growth
18. „The Long Road Ahead to Transition to Post-Quantum Cryptography", https://cacm.acm.org/magazines/2022/1/257440-the-long-road-ahead-to-transition-to-post-quantum-cryptography/fulltext
19. https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/
20. https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization
21. https://safecode.org/blog/preparing-for-post-quantum-cryptography-roadmap-initial-guidance/
22. https://csrc.nist.gov/publications/detail/sp/800-40/rev-4/final

Beteiligte Teams

Beteiligte Teams

Die Daten und Insights in diesem Bericht wurden von einer Gruppe von Sicherheitsexpert*innen bereitgestellt, die in vielen verschiedenen Teams bei Microsoft arbeiten. Ihr gemeinsames Ziel ist es, Microsoft, seine Kund*innen und die ganze Welt vor der Bedrohung durch Cyberangriffe zu schützen. Diese Insights teilen wir ganz nach unserer Maßgabe der Transparenz und mit dem gemeinsamen Ziel, die Welt zu einem sichereren Ort für alle zu machen.

AI for Good Research Lab: Nutzt die Leistungsfähigkeit von Daten und KI, um viele der weltweiten Herausforderungen anzugehen. Das Lab arbeitet mit Organisationen außerhalb von Microsoft zusammen und verbessert die Lebensgrundlagen und die Umgebungen von Menschen mithilfe von KI. Zu den Schwerpunkten zählen Onlinesicherheit (Desinformation, Cybersicherheit, der Schutz von Kindern), Notfallreaktion, Nachhaltigkeit und KI für das Gesundheitswesen.

Azure Edge & Platform, Enterprise & OS Security: Verantwortlich für die zentrale Betriebssystem- und Plattformsicherheit in Windows, Azure und weiteren Microsoft-Produkten. Das Team entwickelt branchenführende Sicherheits- und Hardwarelösungen für Microsoft-Plattformen, um Kompromittierungen in Form von Exploits, Identitätsdiebstahl und Schadsoftware vom Chip bis zur Cloud zu reduzieren. Schöpfer der Secured-Core-Plattform von Microsoft für PC, Edge und Server sowie des Microsoft Pluton-Sicherheitsprozessors und mehr.

Azure Networking, Core: Ein Cloud-Networking-Team, das sich auf die Microsoft WAN- und Rechenzentrumsnetzwerke konzentriert sowie auf die Software-definierte Netzwerkinfrastruktur von Azure, einschließlich der DDoS-Plattform, der Netzwerk-Edge-Plattform und der Netzwerksicherheitsprodukte wie Azure WAF, Azure Firewall und Azure DDoS Protection Standard.

Cloud Security Research Team: Durch den Schutz der Microsoft Cloud, das Entwickeln innovativer Sicherheitsfunktionen und -produkte und durch aktive Forschung schützt dieses Team die Microsoft-Kund*innen und ermöglicht ihnen die sichere Transformation ihrer Organisationen.

Customer Security and Trust (CST): Ein Team, das sich laufend um die Verbesserung der Kundensicherheit in Microsoft-Produkten und -Onlinediensten kümmert. In Kooperation mit Entwicklungs- und Sicherheitsteams aus dem gesamten Unternehmen gewährleistet das CIST Compliance, erhöht die Sicherheit und sorgt für mehr Transparenz, um Kund*innen zu schützen und das globale Vertrauen in Microsoft zu stärken.

Customer Success: Die Sicherheitsteams in Customer Success arbeiten direkt mit den Kund*innen zusammen, um bewährte Methoden, gelernte Lektionen und Handlungsempfehlungen zu teilen, mit denen die Kund*innen die Transformation und Modernisierung ihrer Sicherheit beschleunigen können. Dieses Team sammelt und organisiert bewährte Methoden und Erkenntnisse aus unseren eigenen Verfahren – und aus denen unserer Kund*innen – und überträgt sie in Referenzstrategien, Referenzarchitekturen, Referenzpläne und vieles mehr.

Cyber Defense Operations Center (CDOC): Die Einrichtung für Cybersicherheit und Verteidigung von Microsoft ist ein Fusion Center, in dem Sicherheitsprofis aus dem ganzen Unternehmen zusammenfinden, um unsere Unternehmensinfrastruktur ebenso zu schützen wie die Cloud-Infrastruktur, auf die Kund*innen zugreifen. Incident-Expert*innen sitzen neben Datenwissenschaftler*innen und Sicherheitsingenieur*innen aus allen Dienst-, Produkt- und Gerätesparten von Microsoft, um rund um die Uhr dabei zu helfen, Bedrohungen aufzuspüren, abzuwehren und auf sie zu reagieren.

Democracy Forward Initiative: Ein Microsoft-Team, das daran arbeitet, die Grundlagen der Demokratie zu bewahren, zu schützen und voranzubringen. Dazu fördert es eine gesunde Informationsinfrastruktur, schützt offene und sichere demokratische Prozesse und tritt für die zivilgesellschaftliche Verantwortung von Unternehmen ein.

Digital Crimes Unit (DCU): Ein Team aus Anwält*innen, Ermittler*innen, Datenwissenschaftler*innen, Ingenieur*innen, Analyst*innen und Geschäftsexpert*innen, die sich auf globaler Ebene mithilfe von Technologie, Forensik, Zivilklagen, Anzeigen und sowohl öffentlichen als auch privaten Partnerschaften für die Bekämpfung von Cyberkriminalität einsetzen.

Digital Diplomacy: Ein internationales Team aus ehemaligen Diplomat*innen, politischen Entscheidungsträger*innen und Jurist*innen, die sich angesichts nationalstaatlicher Konflikte für einen friedlichen, stabilen und sicheren Cyberspace einsetzen.

Digital Security & Resilienz (DSR): Eine Organisation, die sich auf die Fahnen geschrieben hat, Microsoft zu ermöglichen, die vertrauenswürdigsten Geräte und Dienste zu entwickeln und dabei gleichzeitig die Sicherheit unseres Unternehmens zu gewährleisten und sowohl unsere Unternehmensdaten als auch die Daten unserer Kund*innen zu schützen.

Digital Security Unit (DSU): Ein Team von Anwält*innen und Analyst*innen für Cybersicherheit, die rechtliches, geopolitisches und technisches Fachwissen beisteuern, um Microsoft und seine Kund*innen zu schützen. Die DSU stärkt das Vertrauen in die Enterprise-Abwehrmaßnahmen von Microsoft gegen moderne Gegner im Cyberspace weltweit.

Digital Threat Analysis Center (DTAC): Ein Team aus Expert*innen, die nationalstaatliche Bedrohungen analysieren und über sie berichten, dazu gehören Cyberangriffe und Beeinflussungsoperationen. Das Team kombiniert Informationen und Aufklärung über Cyberbedrohungen mit geopolitischen Analysen, um unsere Kund*innen und Microsoft mit Insights zu versorgen und beide über effektive Reaktionen und Schutzmaßnahmen zu informieren.

Enterprise and Security: Ein Team, das sich auf die Bereitstellung einer modernen, sicheren und verwaltbaren Plattform für Intelligent Cloud und Intelligent Edge konzentriert.

Enterprise Mobility: Ein Team, das den modernen Arbeitsplatz und die moderne Verwaltung vorantreibt, um Daten sowohl in der Cloud als auch On-Premises zu schützen. Endpoint Manager umfasst die Dienste und Tools, die Microsoft und Kund*innen zum Verwalten und Überwachen von mobilen Geräten, Desktopcomputern, virtuellen Maschinen, eingebetteten Geräten und Servern verwenden.

Beteiligte Teams

Fortsetzung

Enterprise Risk Management: Ein Team, das über Geschäftsbereiche hinweg arbeitet, um Risikodiskussionen mit der Führungsebene von Microsoft zu priorisieren. Das ERM vernetzt mehrere operative Risikoteams, verwaltet das Microsoft-Risikoframework für Unternehmen und erleichtert die interne Sicherheitsbewertung des Unternehmens mithilfe des NIST Cybersecurity Framework.

Global Cybersecurity Policy: Ein Team, das mit Regierungen, NGOs und Branchenpartnern zusammenarbeitet, um die öffentliche Debatte über Cybersicherheit zu fördern, denn dadurch können Kund*innen ihre Sicherheit und Resilienz bei der Einführung von Microsoft-Technologie stärken.

Identity and Network Access (IDNA) Security: Ein Team, das alle Microsoft-Kund*innen vor unbefugtem Zugriff und Betrug schützt. IDNA Security ist ein interdisziplinäres Team aus Ingenieur*innen, Produktmanager*innen, Datenwissenschaftler*innen und Sicherheitsermittler*innen.

M365 Security: Organisation, die Sicherheitslösungen wie Microsoft Defender for Endpoint (MDE), Microsoft Defender for Identity (MDI) und andere entwickelt, um Geschäftskunden zu schützen.

Microsoft AI, Ethics and Effects in Engineering and Research (AETHER): Ein Beratungsgremium bei Microsoft, das sicherstellt, dass neue Technologien verantwortungsvoll entwickelt und in die Praxis eingeführt werden.

Microsoft Bing Search and Distribution: Ein Team, das sich auf die Bereitstellung einer erstklassigen Internetsuchmaschine spezialisiert hat und Benutzer*innen auf der ganzen Welt ermöglicht, schnell zuverlässige Suchergebnisse und Informationen zu finden, einschließlich der Verfolgung von Themen und angesagten Storys, die für sie relevant sind, und ihnen gleichzeitig die Kontrolle über ihre Privatsphäre in die Hand gibt.

Microsoft Customer and Partner Solutions: Die zentrale kommerzielle Go-to-Market-Geschäftseinheit bei Microsoft, die Positionen wie Sicherheits- und technische Vertriebsspezialist*innen und Berater*innen vereint.

Microsoft Defender Experts: Die größte globale Microsoft-Organisation mit produktzentrierten Sicherheitsforscher*innen, Expert*innen für angewandte Wissenschaft und Threat Intelligence-Analyst*innen. Die Defender Experts entwickeln innovative Erkennungs- und Bekämpfungsfunktionen für die Sicherheitsprodukte in Microsoft 365 und die Microsoft Defender Experts Managed Services.

Microsoft Defender for IoT: Ein Team aus Spitzenforscher*innen auf ihrem Gebiet, das sich auf Reverse-Engineering von IoT-/OT-Schadsoftware, -Protokolle und -Firmware spezialisiert hat. Das Team verfolgt IoT-/OT-Bedrohungen, um bösartige Trends und Kampagnen aufzudecken.

Microsoft Defender Threat Intelligence (RiskIQ): Ein Team, das taktische Aufklärung betreibt, indem es die umfangreiche Sammlung von Microsoft an externer Telemetrie analysiert, die sich entwickelnde Bedrohungslandschaft kartiert, um bis dato unbekannte Bedrohungsinfrastruktur zu entdecken, und Kontext zu Akteuren und Kampagnen hinzufügt. Das Team veröffentlicht regelmäßig aktuelle und spezifische Forschungsergebnisse, um die Verteidiger mit entscheidender taktischer Aufklärung zu versorgen.

Microsoft Security Business Development Team: Ein Team, das die Wachstumsstrategie, die Partnerschaften und die strategischen Investitionen von Microsoft in Bezug auf die Cybersicherheit leitet.

Microsoft Security Response Center (MSRC): Ein Team, das mit Sicherheitsexpert*innen zusammenarbeitet, um die Kund*innen sowie die Partnerinfrastruktur von Microsoft zu schützen. Das MSRC ist ein integraler Bestandteil des Cyber Defense Operations Centers (CDOC) von Microsoft. Es vereint Expert*innen für Sicherheitsmaßnahmen, um Bedrohungen zu erkennen sowie in Echtzeit darauf zu reagieren.

Microsoft Security Services for Incident Response: Ein Team von Expert*innen für Cybersicherheit, das Kund*innen während des gesamten Cyberangriffs zur Seite steht – von der Ermittlung bis hin zur erfolgreichen Eindämmung und Aktivitäten zur Wiederherstellung. Die Dienste werden über zwei eng integrierte Teams angeboten: das Detection and Response Team (DART) mit dem Schwerpunkt auf der Untersuchung und den Grundlagen für eine Wiederherstellung und das Compromise Recovery Security-Team (CRSO), das sich auf Eindämmungs- und Wiederherstellungsaspekte konzentriert.

Microsoft Theft Intelligence Center (MSTIC): Ein Team, das sich auf die Identifizierung, die Nachverfolgung und das Sammeln von Informationen über die raffiniertesten Gegner konzentriert, die gegen Microsoft-Kund*innen aktiv sind. Dies umfasst nationalstaatliche Bedrohungen, Schadsoftware und Phishing.

One Engineering System (1ES): Ein Team mit der Aufgabe, erstklassige Tools bereitzustellen, die Microsoft-Entwickler*innen helfen, so produktiv und sicher wie möglich zu arbeiten. Das Team leitet die zentrale Strategie für die Absicherung der durchgängigen Softwarelieferkette von Microsoft.

Operational Threat Intelligence Center (OpTIC): Dieses Team ist verantwortlich für die Verwaltung und Weiterverbreitung von Erkenntnissen über Cyberbedrohungen, die die Aufgabe des Microsoft Cyber Defense Operation Centers (CDOC) unterstützen, Microsoft und unsere Kund*innen zu schützen.

Microsoft

Zur Beleuchtung der Bedrohungslandschaft und Unterstützung einer digitalen Verteidigung

- Mehr erfahren: **https://microsoft.com/mddr**
- Hintergründe entdecken: **https://blogs.microsoft.com/on-the-issues/**
- In Verbindung bleiben: **@msftissues und @msftsecurity**