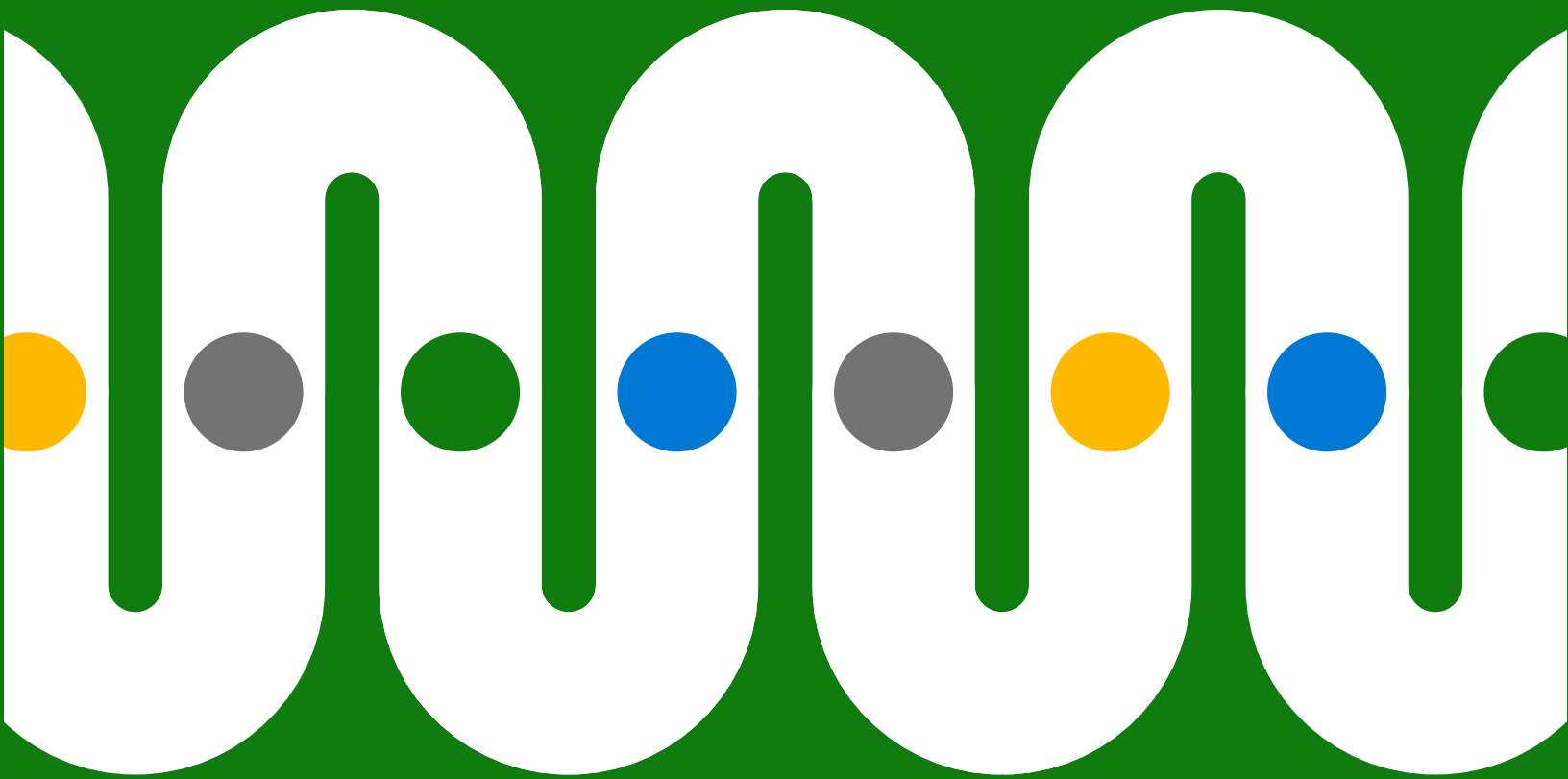
Microsoft Security

In drei Schritten zum lückenlosen Datenschutz



Inhaltsverzeichnis

Einleitung

Bei einer Umfrage unter Compliance-Entscheidungstragenden zeigten sich 95 % hinsichtlich der Herausforderungen im Bereich Datenschutz besorgt.[2]

Unternehmen haben ihre digitale Präsenz durch hybrides Arbeiten massiv und auf eine Weise ausgebaut, die weit über die herkömmlichen Grenzen des Büros hinausgeht.

Dies allerdings hat zu mehr Datenfragmentierung und -exfiltration geführt – noch verkompliziert durch das schnelle Wachstum bei zahlreichen Anwendungen, Geräten und Standorten. Viele Mitarbeitende haben auf der Suche nach größerer Erfüllung oder Flexibilität außerdem die Stelle gewechselt, was die Herausforderungen noch vergrößert hat. Nicht zuletzt sind dadurch auch neue blinde Flecken in den ständig wachsenden Datenbeständen entstanden.[1]

All diese Faktoren haben CIOs und CISOs dazu veranlasst, ihren Ansatz in Bezug auf den Informationsschutz zu überdenken. Bei einer Umfrage unter mehr als 500 US-amerikanischen Compliance-Entscheidungstragenden zeigten sich fast alle (95 %) hinsichtlich der Herausforderungen im Bereich Datenschutz besorgt.[2]

[1] „How Microsoft can help reduce insider risk during the Great Reshuffle", Alym Rayani, Microsoft Security, 28. Februar 2022

[2] September 2021 – Umfrage unter 512 US-amerikanischen Compliance-Entscheidungstragenden von Vital Findings im Auftrag von Microsoft.

Die IT- und Sicherheitsteams sind auf der Suche nach besseren Möglichkeiten, den gesamten Datenlebenszyklus über Multi-Cloud, Hybrid Cloud- und On-Premises-Umgebungen hinweg zu verwalten. Dieser End-to-End-Ansatz umfasst drei wichtige Schritte:

Schritt 1: Daten identifizieren

Finden Sie heraus, wo Ihre Daten gespeichert sind, um welche Art von Daten es sich handelt und wie sie verwendet oder freigegeben werden.

Schritt 2: Daten klassifizieren

Klassifizieren und kennzeichnen Sie Ihre Daten, damit Sie die richtigen Richtlinien und Maßnahmen zur Risikominderung anwenden können.

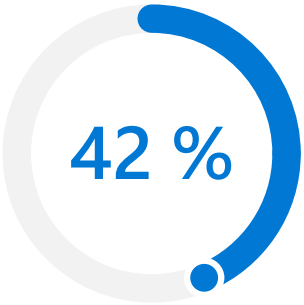
Schritt 3: Datenverluste verhindern

Sorgen Sie für ein Gleichgewicht zwischen Risikominimierung und Flexibilität für Ihre Mitarbeitenden durch eine intelligente Erkennung und Kontrolle.

Das Ziel dieses Ansatzes? Lücken schließen und Risiken minimieren – ohne die Produktivität zu beeinträchtigen.

Schritt 1

Daten identifizieren



Auf die Frage, wie viele ihrer Daten „im Dunklen“ liegen, gaben 42 % der Unternehmen an, dass dies mindestens auf die Hälfte ihrer Daten zutrifft.[3]

Diese „versteckten“ Daten können in verschiedensten Formen vorliegen: von E-Mail-Anhängen und Kundengesprächsdaten bis hin zu Maschinen-protokollen und Videoaufnahmen.

Wenn Sie Ihre Daten nicht identifizieren können, das heißt, wenn Sie nicht wissen, wo sich all Ihre Daten befinden, um welche Arten von Daten es sich handelt oder wie diese verwendet und freigegeben werden, ist es unmöglich, die richtigen Schutzebenen oder Richtlinien auf die Daten anzuwenden.

Von modernen Unternehmen werden ständig riesige Datenmengen generiert. Hierbei handelt es sich nicht nur um Dokumente, E-Mails und Nachrichten, sondern um alle möglichen Daten – von Videomaterial von Sicherheitskameras bis hin zu Geolocation-Daten. Durch die weite Verbreitung von Anwendungen, Geräten und Speicher, ob lokal oder in der Cloud, wird dieses Problem noch verschärft.

Die Identifizierung all dieser Daten kann schwierig sein. 42 % der Unternehmen geben an, dass mindestens die Hälfte ihrer Daten „im Dunklen“ liege.[3] So werden Informationen bezeichnet, die zwar erfasst wurden, aber nicht bekannt sind oder nicht für geschäftliche Zwecke genutzt werden. Manchmal werden Daten „dunkel“, wenn Mitarbeitende, die sie erstellt haben, das Projekt oder gar die Stelle wechseln. Und oft gibt es einfach keine Systeme, um die Daten zum Zeitpunkt der Erstellung oder Änderung zu identifizieren.

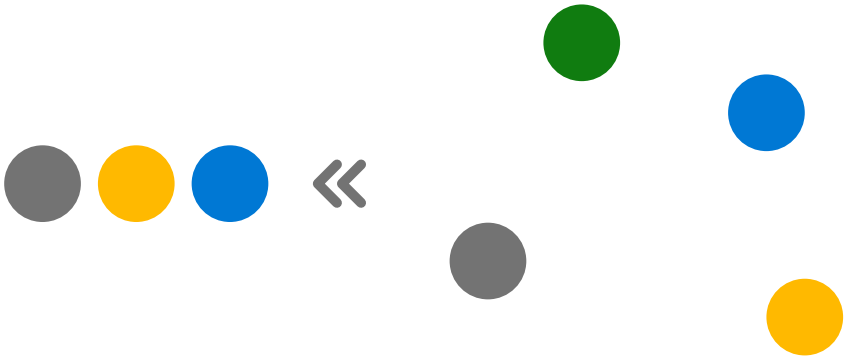
[3] „2022 State of Data Governance and Empowerment Report“, Enterprise Strategy Group, Juli 2022

Möchten Sie einen durchgängigen Discovery-Workflow auf einer Plattform entwickeln?

Erfahren Sie mehr über die Datenermittlung von Microsoft Purview auf **Microsoft.com**.

Diese Herausforderung wird sich noch verstärken. Die Menge an neuen Daten, die erstellt, erfasst, repliziert und konsumiert werden, wird sich bis 2026 voraussichtlich mehr als verdoppeln, wobei Unternehmensdaten mehr als zweimal so schnell wachsen wie Verbraucherdaten.[4]

Künstliche Intelligenz (KI) und Machine Learning (ML) können dabei helfen, sensible Daten wie E-Mail-Adressen, Gesundheitsdaten, Kreditkartennummern oder geistiges Eigentum zu erkennen und automatisch zu klassifizieren. KI und ML können auch die Genauigkeit bei der Klassifizierung erhöhen und Daten rückwirkend überprüfen. Diese Erkennungsprozesse können auf Ihre gesamten Datenbestände ausgeweitet werden, mit entsprechender Cloud-übergreifender Aufbewahrung, Erfassung, Analyse und Überprüfung sowie Exporten.



[4] „Worldwide IDC Global DataSphere Forecast, 2022–2026: Enterprise Organizations Driving Most of the Data Growth", John Rydning, IDC, Mai 2022

Schritt 2

Daten klassifizieren

Die Klassifizierungen und Richtlinien müssen den Daten „auf ihrer Reise“ folgen.

Wenn Mitarbeitende beispielsweise Kreditkartennummern aus einem Microsoft Word-Dokument in eine Excel-Tabelle kopieren, sollten Klassifizierung und Richtlinien automatisch auf beide Dokumente angewendet werden.

Möchten Sie sensible Daten in Ihrer Umgebung besser verwalten und schützen?

Erfahren Sie mehr über die Klassifizierung und den Schutz Ihrer Daten mit Microsoft Purview auf **Microsoft.com**.

Eine ordnungsgemäße Datenklassifizierung hilft Ihnen dabei, die richtigen Richtlinien und Maßnahmen zur Eindämmung der Risiken zu ermitteln, damit Sie sicherstellen können, dass verschiedene Arten von Daten nicht versehentlich oder vorsätzlich missbraucht werden oder ohne Befugnis darauf zugegriffen wird. Schutzmaßnahmen wie Verschlüsselung und Wasserzeichen können zusätzlichen Schutz für Daten im Ruhezustand, bei der Übertragung und während ihrer Nutzung bieten.

Die Klassifizierungsmaßnahmen und Richtlinien müssen jedoch den Daten im gesamten Unternehmen folgen. Kennzeichnungs- und Schutzrichtlinien können nicht auf einzelne Dokumente beschränkt werden, sondern müssen Ihre gesamten digitalen Ressourcen umfassen – von On-Premises- oder Cloud-basierten Repositorys über Software-as-a-Service (SaaS)-Apps bis hin zu betriebssystemnativen Anwendungen.

Bei herkömmlichen Ansätzen ist die Klassifizierung all dieser Daten mit einem großen manuellen Aufwand verbunden. Dabei kann es zu Fehlern kommen, oder wichtige Daten werden übersehen. Integrierte und trainierbare Klassifizierungslösungen können dazu beitragen, diesen Prozess zu automatisieren. Nicht zuletzt ermöglicht eine solche integrierte Lösung es den Administrator*innen, Richtlinien zentral und systemübergreifend zu verwalten.

Schritt 3

Datenverluste verhindern

DLP-Richtlinien können Aktionen verhindern, die nicht Compliance-konform sind.

Wenn Mitarbeitende z. B. versuchen, eine Tabelle mit Kreditkartennummern auf einen USB-Stick herunterzuladen oder in den Cloud-Speicher hochzuladen, könnte die DLP-Richtlinie diese Aktivität als nonkonform identifizieren und sie verhindern.

Möchten Sie sensible Informationen auf intelligente Weise erkennen und kontrollieren?

Erfahren Sie mehr über Data Loss Prevention mit Microsoft Purview auf **Microsoft.com**.

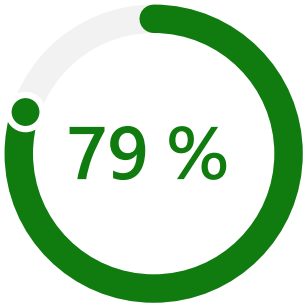
Nachdem Sie Ihre Daten identifiziert und klassifiziert haben, können Data Loss Prevention (DLP)-Lösungen durchgängige Schutzrichtlinien erzwingen, die Bedrohungen wie „dunkle" Daten und Datenexfiltrationen reduzieren, sodass aktuelle und ehemalige Mitarbeitende weder absichtlich noch versehentlich vertrauliche Daten ohne entsprechende Befugnis freigeben, offenlegen oder übertragen können.

Intelligente DLP-Lösungen verwenden Kontextinformationen, um ein Gleichgewicht zwischen Flexibilität einerseits und der Blockierung von Aktionen mit hohem Risiko andererseits zu finden. So können Personen z. B. eine Aktion fortsetzen, nachdem sie über potenzielle Risiken und entsprechende Richtlinien aufgeklärt wurden. Dies kann zum Schutz sensibler Daten beitragen, während die Benutzer*innen gleichzeitig geschult werden, damit sie die Risiken besser verstehen.

DLP-Lösungen tragen außerdem zum Schutz von geistigem Eigentum und anderen wichtigen Geschäftsdaten bei und verbessern die Einhaltung von Vorschriften wie der EU-Datenschutz-Grundverordnung (DSGVO), dem Health Information Portability and Accountable Act (HIPAA) und dem California Consumer Privacy Act (CCPA).

Ein umfassender Ansatz zur Verhinderung von Datenverlusten (Data Loss Prevention) sorgt zudem dafür, dass Richtlinien im gesamten Unternehmen konsequent umgesetzt werden, was eine potenzielle Ausnutzung von Schwachstellen im Datenlebenszyklus verringert.

Verwenden Sie keine aufgesetzten Datenschutzlösungen, sondern setzen Sie auf Integration.



Eine Umfrage unter Compliance-Entscheidungstragenden ergab, dass 79 % mehrere Compliance- und Datenschutzprodukte erworben hatten.

Die Mehrheit hatte drei oder mehr gekauft.[5]

Viele Unternehmen haben einen „aufgesetzten" Ansatz für den Informationsschutz ausprobiert und für die Verwaltung einzelner Abschnitte des Datenlebenszyklus mehrere Lösungen verwendet. Dies zwingt jedoch ihre Sicherheits-, Data Governance-, Compliance- und Rechtsabteilung dazu, mit einer Art von Flickenteppich zu arbeiten, der oft ineffektiv ist und die Ressourcen unnötig strapaziert.

Ein integrierter Ansatz kann diese Lücken schließen und Datenidentifizierung und -klassifizierung sowie DLP zusammenführen. Außerdem verkürzt sie die Schulungszeit für Benutzer*innen, die Richtlinienbenachrichtigungen auf vertraute Weise nativ innerhalb der gewohnten Anwendungen erhalten.

[5] Umfrage von Februar 2022 unter 200 US-amerikanischen Compliance-Entscheidungstragenden – (n=100 599–999 Beschäftigte, n=100 1.000+ Beschäftigte) im Auftrag von Microsoft mit MDC Research

Eine integrierte Lösung: Microsoft Purview

Microsoft Purview hilft Ihnen dabei, die Herausforderungen des heute dezentralisierten und datenreichen Arbeitsplatzes zu bewältigen – mit einem umfassenden Portfolio an Lösungen, die Sie beim Steuern, Schützen und Verwalten all Ihrer Datenbestände unterstützen.

Mehr als nur Governance

Erfahren Sie mehr über den Schutz Ihrer Daten mit Microsoft Purview >

Interessieren Sie sich für einen bestimmten Aspekt beim Thema Datenschutz? Erfahren Sie mehr darüber, wie Microsoft Purview Ihnen in folgenden Bereichen helfen kann:

Datenermittlung >

Datenklassifizierung und Datenschutz >

Data Loss Prevention >

Microsoft Security