Reihe „Lösungsleitfaden“

Microsoft

Sicherheit:
Ein Leitfaden für flexible Lösungen

Sicherheitsziele entdecken

Ihre Sicherheit stärken

Die Bedrohungslandschaft entwickelt sich weiter und die Vergrößerung der Angriffsflächen hat zu einer Überforderung der Cybersicherheitsressourcen und zu überlasteten Teams geführt. Deshalb benötigt Ihr Sicherheitsteam flexible Lösungen, die umfassende Informationen über Bedrohungen liefern.

Begegnen Sie den Herausforderungen von heute mit Lösungen, die über Menschen, Geräte, Anwendungen und Daten hinweg integriert sind. Arbeiten Sie einfach plattformübergreifend mit integrierten Umgebungen. Und sichern Sie Ihre Zukunft mit KI und Automatisierung.

Dieser Leitfaden zeigt Ihnen Schritt für Schritt, wie Sie Ihr Unternehmen schützen und gleichzeitig für reibungslose Benutzererlebnisse sorgen, damit die Mitarbeiter*innen ihre Aufgaben erledigen können. Jedes Szenario enthält eine kurze Liste von Fragen, empfohlenen Aktivitäten und Ressourcen für den Einstieg.

Remote-Zugriff absichern

Ermöglichen Sie Remote-Mitarbeiter*innen den Zugriff auf die benötigten Anwendungen überall, jederzeit und mit erhöhter Sicherheit.

Stellen Sie sich folgende Fragen	Empfohlene Aktivitäten
1. Haben Sie eine Möglichkeit, Identitäten für alle Ihre Geräte und Anwendungen zu verwalten?	☐ Verwenden Sie Microsoft Azure Active Directory (Azure AD) als universelle Identitätsplattform.
2. Können sich Ihre Benutzer*innen anmelden und nahtlos auf alle Ihre Geschäftsanwendungen zugreifen?	☐ Verwenden Sie Single Sign-on mit Azure AD, damit Mitarbeiter*innen über jede App oder jedes Gerät auf Ressourcen zugreifen können, während Sie remote arbeiten.
3. Verwenden Sie derzeit Kennwörter für Ihre Authentifizierung?	☐ Verwenden Sie Microsoft Azure Multi-Faktor-Authentifizierung, um die Sicherheit für Remote-Arbeit zu verbessern.
4. Können Sie die Sicherheit auf Ihre Geräte ausdehnen?	☐ Verwalten und schützen Sie Unternehmensdaten in genehmigten Apps auf Mobilgeräten mit Azure AD und Microsoft Endpoint Manager.

Steigen Sie noch heute mithilfe der folgenden Ressourcen ein:

- Starten Sie noch heute mit einem Crashkurs in Azure Active Directory.
- Erfahren Sie mehr über Sicherheit für Remote-Mitarbeiter*innen.
- Beginnen Sie mit dem Einsatz sicherer Lösungen für die Remote-Arbeit.

VPN-Engpässe entschärfen

Ergänzen Sie Ihr bestehendes Netzwerk um neue identitätsbasierte Kontrollen, um Betriebsunterbrechungen und ein erneutes Aufkommen alter Risiken zu verhindern.

Stellen Sie sich folgende Fragen	Empfohlene Aktivitäten
1. Verwalten Sie die Sicherheit aller Cloud-Anwendungen, die Ihr Unternehmen nutzt?	☐ Verfolgen Sie die Cloud Apps Ihres Unternehmens und schützen Sie sie mit Funktionen wie Single-Sign-on und bedingtem Zugriff in Microsoft Cloud App Security und Azure AD.
2. Unterstützen Sie den identitätsbasierten bedingten Zugriff?	☐ Verwenden Sie den bedingten Zugriff im Rahmen von Azure AD.
3. Verwalten Sie die Sicherheit aller Cloud-Anwendungen, die Ihr Unternehmen nutzt?	☐ Verfolgen Sie die Cloud Apps Ihres Unternehmens und schützen Sie sie mit Funktionen wie Single-Sign-on und bedingtem Zugriff in Microsoft Cloud App Security und Azure AD.
4. Wie können Sie auf eine Single-Sign-on Lösung für alle Ihre Anwendungen in der Cloud und On-Premises umsteigen?	☐ Sichern Sie den Zugriff auf Ihre älteren Apps mit dem Azure AD-Anwendungsproxy oder vordefinierten Integrationen mit Netzwerkanbietern und Controllern für die Bereitstellung von Apps.

Steigen Sie noch heute mithilfe der folgenden Ressourcen ein:

- Sehen Sie sich das Webinar Security Controls for Remote Work an.
- Lesen Sie das Whitepaper zu Single Sign-on und zur Zugriffsverwaltung für alle Anwendungen aus der Cloud.
- Erfahren Sie mehr über sichere Remote-Arbeit.

Jetzt einsteigen in Zero Trust

Zero Trust sollte als integrierte Sicherheitsphilosophie dienen. Es ist sowohl eine Reise als auch die Grundlage für sichere Remote-Arbeit.

Stellen Sie sich folgende Fragen	Empfohlene Aktivitäten
1. Verfügen Sie über eine Identitätslösung mit bedingtem Zugriff und Analytics, um die Transparenz zu verbessern?	☐ Überprüfen und sichern Sie jede Identität mit starker Authentifizierung in Ihrer gesamten digitalen Infrastruktur.
2. Wird der Zugriff nur auf über die Cloud verwaltete und Compliance-konforme Geräte gewährt?	☐ Verschaffen Sie sich eine Übersicht über alle Geräte, die auf das Netzwerk zugreifen. Gewährleisten Sie Compliance und Integrität, bevor Sie Zugriff gewähren.
3. Sind Ihre On-Premises-Apps mit Internetzugang und Cloud Apps mit Single-Sign-on konfiguriert?	☐ Entdecken Sie die Schatten-IT, gewähren Sie Zugriff, überwachen und kontrollieren Sie Anwenderaktionen und stellen Sie geeignete In-App-Berechtigungen sicher.
4. Werden Ihre Workloads überwacht und bei ungewöhnlichem Verhalten Warnungen ausgegeben?	☐ Wechseln Sie vom perimeterbasierten Datenschutz zum datengesteuerten Schutz.
5. Verfügen Sie über einen Machine Learning-basierten Bedrohungsschutz und Filterung mit kontextbasierten Signalen?	☐ Verwenden Sie die Telemetrie, um Angriffe und Anomalien zu erkennen, risikoreiches Verhalten automatisch zu blockieren und zu markieren.

Steigen Sie noch heute mithilfe der folgenden Ressourcen ein:

- Testen Sie das Zero Trust Assessment Tool.
- Holen Sie sich zehn Tipps für den Einstieg in Zero Trust.
- Erfahren Sie, wie Sie Zero Trust in Ihrem Unternehmen implementieren können.

Schutz vor Phishing und komplexen Bedrohungen erhöhen

Schützen Sie Ihre Organisation domänenübergreifend vor komplexen Bedrohungen wie Phishing und Zero-Day-Malware.

Stellen Sie sich folgende Fragen	Empfohlene Aktivitäten
1. Haben Sie Sicherheitsfunktionen, die in Ihren E-Mail-Service integriert sind?	☐ Aktivieren Sie die Schutzfunktionen Ihres E-Mail-Services.
2. Haben Sie eine starke Authentifizierungslösung?	☐ Verwenden Sie Microsoft Azure Multi-Faktor-Authentifizierung für alle Ihre Konten, um Ihre Sicherheit zu verbessern.
3. Wissen Sie, wie Sie Phishing-Angriffe erkennen?	☐ Informieren Sie sich selbst, Freunde und Kolleg*innen darüber, wie Sie Phishing-Versuche erkennen und verdächtige Begegnungen melden können.
4. Ist Ihre Lösung für den Schutz von Endpunkten vollständig und automatisiert?	☐ Verwenden Sie Microsoft Defender Advanced Threat Protection für den präventiven Schutz von Endpunkten, die Erkennung nach Verstößen sowie für die automatische Untersuchung und Reaktion.
5. Verfügen Sie über eine integrierte Lösung zum Schutz vor Bedrohungen, mit der Sie alle Bedrohungen in einer zentralen Ansicht anzeigen können?	☐ Analysieren Sie Bedrohungsdaten über Domänen hinweg und erstellen Sie ein vollständiges Bild von jedem Angriff in einem einzigen Dashboard mit Microsoft Threat Protection.

Steigen Sie noch heute mithilfe der folgenden Ressourcen ein:

- Laden Sie das E-Book „Office 365 Advanced Threat Protection“ herunter.
- Nutzen Sie einen modernen Ansatz für den Schutz von Endpunkten.
- Erfahren Sie, wie integrierter Bedrohungsschutz Ihre Sicherheit stärken kann.

Vertrauliche Informationen schützen

Die Notwendigkeit, Daten zu schützen und zu verwalten und Risiken zu handhaben, ist für die digitale Transformation unerlässlich.

Stellen Sie sich folgende Fragen	Empfohlene Aktivitäten
1. Wissen Sie, wo Ihre geschäftskritischen und sensiblen Daten gespeichert sind und wofür sie verwendet werden?	☐ Mithilfe flexibler und intelligenter Klassifizierungsfunktionen können Sie Ihre vertraulichen Daten identifizieren.
2. Wie schützen Sie in Ihrem gesamten digitalen Umfeld Ihre Daten konsistent und ohne Beeinträchtigung der Endanwenderproduktivität?	☐ Schützen Sie Daten in einer hybriden Umgebung mit einer einheitlichen Admin-Konsole.
3. Können Sie diese Daten kontrollieren, wenn sie innerhalb und außerhalb Ihres Unternehmens weitergegeben werden?	☐ Steuern Sie den Zugriff auf nicht verwaltete Geräte, um vollständigen Zugriff, webbasierten Zugriff oder die vollständige Sperrung des Zugriffs zu ermöglichen.
4. Verwenden Sie mehrere Lösungen zum Klassifizieren, Kennzeichnen und Schützen dieser Daten?	☐ Erweitern Sie die Lösung auf Apps und Dienste von Drittanbietern, sodass Sie eine wirklich umfassende Datenschutzlösung erhalten.

Steigen Sie noch heute mithilfe der folgenden Ressourcen ein:

- Erhalten Sie eine Übersicht über Microsoft Information Protection und Governance.
- Erfahren Sie mehr über Microsoft Information Protection-Ankündigungen.
- Lesen Sie das E-Book „Best Practices für den Datenschutz“.

Insiderrisiken mindern

Erkennen Sie kritische Insiderrisiken schnell, ergreifen Sie entsprechende Maßnahmen, und reagieren Sie auf Verstöße gegen den Verhaltenskodex in der gesamten Unternehmenskommunikation.

Stellen Sie sich folgende Fragen	Empfohlene Aktivitäten
1. Wie anfällig ist Ihr Unternehmen für Insiderbedrohungen?	☐ Erstellen Sie Richtlinien zum Insider-Risikomanagement und aktivieren Sie Berechtigungen für das Insider-Risikomanagement und das Überwachungsprotokoll.
2. Welche Arten von Insider-Bedrohungen beunruhigen Sie am meisten?	☐ Mit einem Alert-Dashboard können Sie potenzielle Risiken, einschließlich Diebstahl durch Mitarbeitende, Datenlecks und anstößige Sprache, überprüfen.
3. Können Sie rechtzeitig Verstöße gegen den Verhaltenskodex in der Unternehmenskommunikation ermitteln?	☐ Anpassbare Vorlagen für die Einhaltung von Kommunikationsrichtlinien ermöglichen es Ihnen, Verstöße gegen die Richtlinien des Verhaltenskodex zu identifizieren und zu beheben.
4. Erfüllen Sie aufsichtsrechtliche Anforderungen für die gesamte Unternehmenskommunikation?	☐ Mit einem Alert-Dashboard können Sie potenzielle Risiken, einschließlich Diebstahl durch Mitarbeitende, Datenlecks und anstößige Sprache überprüfen.

Steigen Sie noch heute mithilfe der folgenden Ressourcen ein:

- Erfahren Sie, wie KI und Machine Learning zur Bekämpfung von Insider-Risiken eingesetzt werden können.
- Starten Sie noch heute mit dem Insider-Risikomanagement.
- Bleiben Sie auf dem Laufenden mit unserem Blog zu Insider-Risiken.

Steigern Sie die Flexibilität und verbessern Sie Ihre Cybersicherheit

Operative Flexibilität kann nicht ohne echtes Engagement und Investitionen in die Cybersicherheit erreicht werden. Globale Unternehmen müssen einen Zustand erreichen, in dem ihre Kerngeschäfte und -dienste nicht durch geopolitische oder sozioökonomische Ereignisse, Naturkatastrophen oder Cyber-Vorfälle gestört werden, wenn sie solche Vorfälle überstehen und stark bleiben möchten.

Die Sicherheitslösungen von Microsoft unterstützen Ihr Unternehmen, indem sie Flexibilität und eine nahtlose User Experience zusammen mit integriertem, erstklassigen Schutz bieten.

Wenn Sie mehr darüber erfahren möchten, wie Microsoft Security Ihr Unternehmen stärken kann, helfen Ihnen unsere Vertriebsberater*innen gerne weiter.

Nehmen Sie Kontakt auf