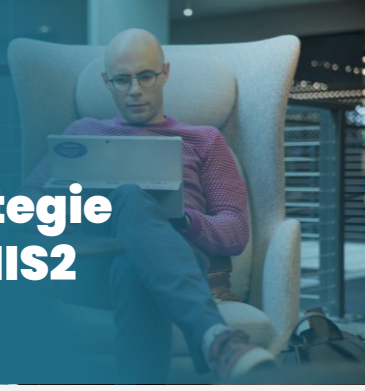
ZUB IT

Microsoft



Stärkung Ihrer Cybersicherheitsstrategie als Vorbereitung auf NIS2

Die europäische Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS2) führt neue Maßnahmen ein, um sicherzustellen, dass Organisationen, die in oder mit der Europäischen Union (EU) tätig sind, über ein hohes gemeinsames Maß an Netz- und Infrastruktursicherheit verfügen.

Die „Richtlinie" umreißt die Ziele, die alle EU-Mitgliedsstaaten erreichen müssen. Jedes Land muss sie in sein eigenes Recht umsetzen, wobei Raum für einige nationale Besonderheiten bleibt, um diese Ziele bis spätestens im Frühjahr 2025 zu erreichen. Richtlinien sind verbindlich in Bezug auf die Mindestanforderungen, die umgesetzt werden müssen.

Als Technologieanbieter, der sich auf Sicherheit konzentriert, verstehen wir die Herausforderungen, die NIS2 für Sie und Ihr Unternehmen mit sich bringt. Wir können Ihnen dabei helfen.

Microsoft Security-Lösungen, die Sie bei der Erfüllung der NIS2-Anforderungen unterstützen

NIS2 legt einen Grundstock an Maßnahmen für das Risikomanagement im Bereich der Cybersicherheit und an Meldepflichten fest. Die gute Nachricht ist, dass die NIS2-Konformität auf die gleichen Zero-Trust-Prinzipien abgestimmt ist, die von Microsoft Security-Lösungen berücksichtigt werden, was zu einem soliden Schutz vor Cyberangriffen auf der gesamten Angriffsfläche beitragen kann.

E-Mail	Endpunkte	Identitäten	Cloud-Workloads	Cloud-Apps
Phishing	Nicht verwaltete Geräte	Anmeldeinformationen für Konten	Gestoppte Dienste	App-Zugriff
URL-Links	Dateiverschlüsselung	Infrastruktur	Gelöschte Backups	Datenexfiltration
Anhänge	Kompromittierte Daten	Workload-Identitäten	Dateiverschlüsselung	

Eine integrierte Sicherheitsstrategie

Der Schlüssel zu einem wirksamen Schutz vor Cyberangriffen liegt in der Wahl der richtigen Systeme für Security Information and Event Management (SIEM) und eXtended Detection Response (XDR). Mit Microsoft erhalten Sie einen vollständig integrierten Sicherheitsansatz und eine optimierte Untersuchung von Sicherheitsbedrohungen und entsprechende Reaktionen.

Microsoft Sentinel

Verschaffen Sie sich Transparenz und verwalten Sie Bedrohungen in Ihrem gesamten digitalen Bestand mit einem modernen SIEM.

\+

Microsoft XDR

Stoppen Sie Angriffe und koordinieren Sie die Reaktion aller Assets mit XDR, das in Microsoft 365 und Azure integriert ist

Microsoft Defender XDR Threat Intelligence

Erkennen und beseitigen Sie moderne Bedrohungen mithilfe dynamischer Cyber-Bedrohungsdaten.

Wie kann Microsoft Security dabei helfen?

1. Vorbeugen

- Branchenführender Ransomware-Schutz
- Bedrohungsbasierte Konfigurationsempfehlungen
- KI und maschinelles Lernen stoppen Bedrohungen automatisch

2. Auffinden

- KI-gesteuerte Erkennung stoppt die weitere Ausführung sofort
- Funktioniert über Geräte, Identitäten, Apps, E-Mails, Daten und Cloud Workloads hinweg

3. Reagieren

- Eine einheitliche Untersuchungs- und Behebungserfahrung
- Ein zentrales Befehls- und Kontrollzentrum mit Microsoft Sentinel
- Schnelle Wiederaufnahme der Arbeit dank automatisierter Datensicherung

Aufbruch zu NIS2-Maßnahmen

- Risikoanalyse
- MFA
- Verschlüsselung
- Training

- Sicherheit in der Lieferkette
- Netzwerksicherheit

- Umgang mit Vorfällen
- Sicherheitsüberwachung

Schützen Sie Ihr Unternehmen Microsoft Security vor Cyberangriffen und Nichterfüllung

72%

verringerte Wahrscheinlichkeit eines Verstoßes

50%

Steigerung der Effizienz von IT- und Sicherheitsteams

25%

reduzierte Kosten für Sicherheitslizenzen

Quelle: Eine in Auftrag gegebene Studie, die von Forrester Consulting durchgeführt wurde, „The Total Economic Impact™ Of Microsoft Security", Februar 2023. Die Ergebnisse beziehen sich auf eine zusammengesetzte Organisation.

Wir erleichtern Ihnen den Einstieg.

Als Microsoft-Partner mit jahrelanger Erfahrung in der Bereitstellung von Sicherheitslösungen möchten wir, dass Sie den bestmöglichen Sicherheitsschutz erhalten, um Ihr Unternehmen zu schützen und die bevorstehende NIS2-Konformitätsfrist einzuhalten. Wir unterstützen Sie.

Sprechen wir darüber, wie wir Ihnen umsetzbare nächste Schritte bieten können.

Kontaktieren Sie uns noch heute