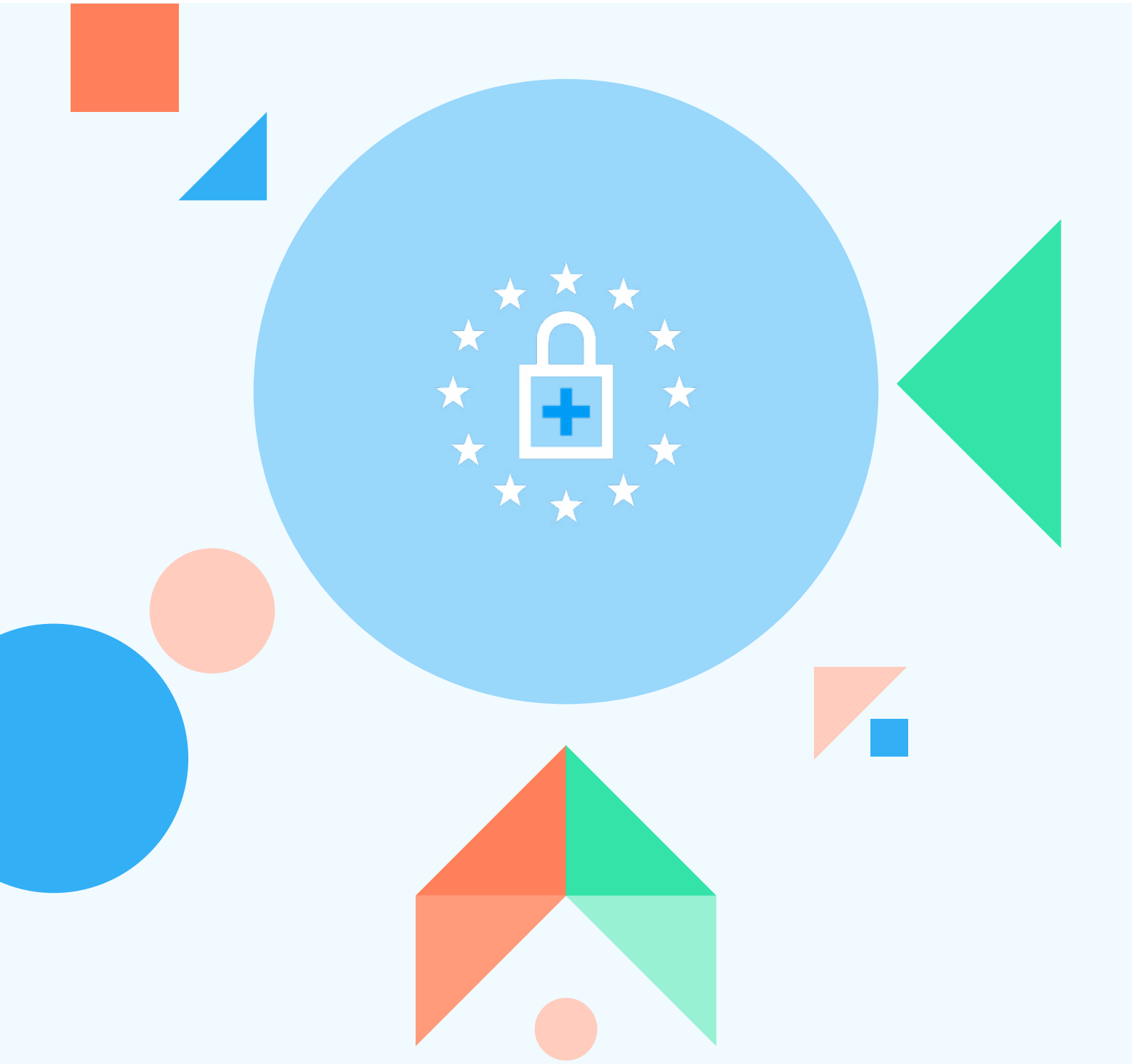
plusserver

Checkliste für NIS2

Ein Leitfaden zur Umsetzung der Security-Richtlinie

Whitepaper



Inhalt

Die Europäische Union hat in den letzten Jahren verstärkte Maßnahmen zur Verbesserung der Cybersecurity in Europa ergriffen. Die Network and Information Security Directive 2 (NIS2) ist ein bedeutender Schritt in diese Richtung. Diese Richtlinie verlangt von Organisationen, dass sie ihre Sicherheitsmaßnahmen verstärken, um die digitale Infrastruktur in der EU vor Cyberbedrohungen zu schützen. Die Umsetzung in nationales Recht hat dabei bis zum 17. Oktober 2024 zu erfolgen. Erfahren Sie im Folgenden, worum es in dieser Richtlinie geht, wer betroffen ist, welche Vorgaben sie enthält und welche Empfehlungen wir für die Umsetzung geben.

Worum geht es bei NIS2?

NIS2 ist eine Erweiterung der ursprünglichen NIS-Richtlinie, die darauf abzielt, die Widerstandsfähigkeit und Sicherheit der digitalen Infrastruktur in der EU zu stärken. NIS2 soll sicherstellen, dass Unternehmen und Organisationen in kritischen Sektoren angemessene Sicherheitsmaßnahmen umsetzen, um Cyberangriffe zu verhindern und effektiv darauf zu reagieren. Sie soll zudem eine verstärkte Zusammenarbeit zwischen den EU-Mitgliedstaaten schaffen, um die europäische Cybersicherheit zu fördern.

Warum braucht es eine solche Richtlinie?

Die Kehrseite der fortschreitenden Digitalisierung ist die steigende Bedrohung durch Cyberkriminalität. Die vom Digitalverband Bitkom ermittelten Schäden durch Cyberkriminalität in Deutschland belaufen sich laut Wirtschaftsschutzbericht 2022 auf 203 Milliarden Euro. Doch nicht nur die Wirtschaft, sondern auch kritische Infrastrukturen (KRITIS) oder öffentliche Einrichtungen sind – unter anderem bedingt durch die politische Lage – heute einem erheblichen Risiko durch Cyberkriminalität ausgesetzt. Der Ausfall kritischer Einrichtungen und Dienste kann schwerwiegende Folgen für das Funktionieren unserer Gesellschaft, der Wirtschaft und der öffentlichen Sicherheit haben.

Wen betrifft NIS2?

Entscheidend ist die Größe bzw. der Umsatz. Unternehmen mit mindestens 50 Mitarbeiter:innen und einem Jahresumsatz/Bilanzsumme von mehr als 10 Millionen Euro können in den Anwendungsbereich der NIS2-Richtlinie fallen, wenn sie gleichzeitig zu den betroffenen Sektoren gehören. Es gibt jedoch Ausnahmen von dieser Größenklassifizierung, z. B. wenn ein Unternehmen kritische Tätigkeiten ausübt, Auswirkungen auf die öffentliche Ordnung hat oder systemische Risiken und grenzüberschreitende Auswirkungen im Falle einer Insolvenz bestehen. In diesen Fällen kann das Unternehmen unter die festgelegten Grenzen, aber dennoch in den Geltungsbereich von NIS2 fallen.

Umgekehrt gibt es auch Kriterien, die Unternehmen von der NIS2-Verordnung ausschließen. Zu diesen Ausnahmen gehören Unternehmen in den Bereichen Verteidigung, nationale Sicherheit, öffentliche Sicherheit und Strafverfolgung. Auch die Justiz, Parlamente und Zentralbanken sind vom Anwendungsbereich ausgenommen.

Übersicht der betroffenen Sektoren nach NIS2

Wesentliche Sektoren	Wichtige Sektoren
Energie	Post- und Kurierdienste
Verkehr und Transport	Abfallwirtschaft
Bankwesen und Finanzmärkte	Produktion, Herstellung und Handel mit chemischen Stoffen
Gesundheitswesen	Produktion, Verarbeitung und Handel von Lebensmitteln
Trinkwasser	Verarbeitendes Gewerbe, Herstellung von Waren
Abwasser	Anbieter digitaler Dienste
Digitale Infrastruktur	Forschungseinrichtungen
ITK-Services (B2B)	
Öffentliche Verwaltung	
Weltraum	

Was sind die Vorgaben der NIS2-Richtlinie?

Die Mitgliedstaaten müssen die Richtlinie bis zum 17. Oktober 2024 in nationales Recht übertragen. Danach muss die EU-Kommission die Anwendung der Richtlinie regelmäßig überprüfen und dem Parlament und dem Rat erstmals bis zum 17. Oktober 2027 Bericht erstatten.

Für betroffene Organisationen legt die NIS2-Richtlinie verschiedene Verpflichtungen fest:

1. Meldepflicht für Zwischenfälle
Organisationen müssen erhebliche Cyberincidents innerhalb von 72 Stunden an die nationalen Behörden melden. Dies ermöglicht es den Behörden, schnell auf Bedrohungen zu reagieren und die Auswirkungen zu minimieren.

2. Sicherheitsmaßnahmen
Unternehmen und öffentliche Verwaltungen müssen geeignete technische und organisatorische Maßnahmen zur Gewährleistung der Cybersecurity umsetzen. Dies umfasst die Sicherung von Netzwerken und Systemen sowie die Implementierung von Sicherheitsrichtlinien.

3. Verantwortung der Geschäftsführung
Die Geschäftsführung ist dazu angehalten, die Umsetzung der Maßnahmen zu überwachen. Dabei haftet sie für Verstöße. Die Teilnahme an entsprechenden Schulungen ist verpflichtend und diese müssen auch den Mitarbeitenden angeboten werden.

Sicherheitsmaßnahmen nach NIS2

Policies	Richtlinien für Risiken und Informationssicherheit
Incident Management	Prävention, Detektion und Bewältigung von Cybervorfällen
Business Continuity	BCM mit Backup Management, Disaster Recovery, Krisenmanagement
Supply Chain	Sicherheit in der Lieferkette
Einkauf	Beschaffung von IT- und Netzwerksystemen
Effektivität	Vorgaben zur Messung von Cyber- und Risikomaßnahmen
Training	Cybersecurity-Hygiene
Kryptographie	Vorgaben für Kryptographie und – wo möglich – Verschlüsselung
Personal	HR-Security
Zugangskontrolle	Zugriffskontrolle
Asset Management	Information Security Management System (ISMS)
Authentifizierung	Einsatz von Multi-Faktor und SSO
Kommunikation	Sichere Kommunikationstools
Notfallkommunikation	Einsatz gesicherter Systeme (Sprache, Video und Text)

Sanktionen bei Verstößen

Bei Verstößen gegen die NIS2-Richtlinie (Risikomanagementmaßnahmen, Art. 21 und Meldepflicht, Art. 23) können Geldstrafen und andere Sanktionen verhängt werden. Die Pflichten der wesentlichen und wichtigen Sektoren (s. Übersicht oben) sind grundsätzlich gleich, jedoch unterscheiden sie sich in der Intensität der Überwachung und der Höhe der Bußgelder bei Nichteinhaltung. Es drohen Höchstbeträge von mindestens zehn bzw. sieben Millionen Euro bzw. zwei Prozent oder eins Komma vier Prozent des weltweiten Umsatzes im Vorjahr.

Welche Rolle spielt der „Stand der Technik“?

Der Stand der Technik im Bereich der Cybersicherheit ist dynamisch und entwickelt sich aufgrund neuer Bedrohungen, technologischer Entwicklungen und bewährter Verfahren ständig weiter. Daher erfordert dessen Einhaltung, dass Unternehmen ihre Sicherheitsmaßnahmen regelmäßig überprüfen, aktualisieren und anpassen, um den aktuellen Herausforderungen und Standards gerecht zu werden.

Die Anforderung, dem Stand der Technik zu entsprechen, ist ein wesentlicher Aspekt der NIS2-Richtlinie. Damit wird sichergestellt, dass Organisationen wirksam auf aktuelle und zukünftige Bedrohungen reagieren und die Integrität ihrer digitalen Infrastruktur gewährleisten können.

Was empfehlen wir bei plusserver?

Klären Sie zunächst, ob Ihre Organisation von NIS2 betroffen ist. Dazu können Sie die Übersicht der Sektoren nutzen und zusätzlich die folgenden Fragen beantworten:

- Erbringt Ihre Organisation Dienstleistungen in der EU oder übt ihre Tätigkeiten in der EU aus?
- Haben Sie mindestens 50 Mitarbeitende oder mindestens 10 Millionen Euro Umsatz und mindestens 10 Millionen Euro Bilanz?
- Treffen Ausnahmeregelungen (s. oben) auf Ihre Organisation zu?

plusserver-Lösungen, die bei der Umsetzung von NIS2 unterstützen

Security-Beratung/ Consulting
- plusserver und Partner-Ökosystem
- Feinkonzeption und Design von Security-Maßnahmen und Architekturen
- Pentests und Audits

Security-Lösungen
- SOC as a Service
- EDR as a Service
- Schwachstellenmanagement
- Next Gen Firewall
- DDoS-Schutz
- Backup/Disaster Recovery

Zertifizierte Infrastruktur
- Standorte in DE
- ISO 27001
- BSI C5 (Typ-II)

Sie sind betroffen? Die folgende Checkliste kann Ihnen helfen, Ihr Unternehmen auf NIS2 vorzubereiten. Die passenden plusserver-Lösungen finden Sie über den Farbcode.

- **Policies/Risikobewertung:** Überprüfen Sie Ihre Strategien zur Risikoanalyse und zur Sicherheit von Informationssystemen. Führen Sie regelmäßige Risikobewertungen durch, um die spezifischen Bedrohungen und Schwachstellen Ihres Unternehmens zu identifizieren.
- **Incident-Management:** Schaffen Sie die Grundlage für eine wirkungsvolle Prävention, Detektion und Bewältigung von Cybervorfällen. Dazu gehören eine Analyse und Bestandsaufnahme der Unternehmensrisiken, die Planung risikobasierter Schutzmaßnahmen bis hin zur vollumfänglichen Überwachung der Infrastruktur (24/7). Um Anomalien frühzeitig zu erkennen, eignet sich beispielsweise eine EDR-Lösung (Endpoint Detection & Response). Dateizugriffe, Prozesse und Netzwerkzugriffe in der gesamten IT-Infrastruktur werden in Echtzeit überwacht und auf auffälliges Verhalten hin analysiert. Ein Security Operations Center (SOC) kann schließlich als zentrale Stelle für die Bündelung und Analyse von Sicherheitsmeldungen verschiedener Schnittstellen dienen. Mit entsprechenden Handlungsempfehlungen, welche durch das SOC bereitgestellt werden, lassen sich Cybervorfälle proaktiv abwehren.
- **Business-Continuity-Management:** Setzen Sie eine Disaster-Recovery-Strategie mit Wiederstellung, z. B. mittels Cloud-Ressourcen, um. Für Ihre externe Backup- und DR-Umgebung sind dieselben Security-Regularien zu beachten wie für externe Cloud-Ressourcen. Bei der Erfüllung unterstützt Sie ein Cloud-Anbieter wie plusserver, bei dem Ihre Daten KRITIS-konform untergebracht sind. Da durch Ransomware prinzipiell auch Backups unbrauchbar gemacht werden können, bietet sich die Nutzung unveränderlicher (immutable) Backups an, um geschäftsfähig zu bleiben. Auch Storage-Funktionen wie Object Lock (etwa beim plusserver S3 Storage) unterstützen Sie dabei, kritische Daten vor jeglicher Manipulation zu schützen.
- **Supply-Chain-Management:** Ebenso relevant wie Ihre eigenen Sicherheitsmaßnahmen ist die NIS2-Compliance Ihrer Zulieferer, inklusive Softwarehersteller und Infrastruktur-Provider. Achten Sie besonders auf Zertifizierungen wie ISO 27001 sowie bei Cloud-Anbietern auf ein BSI-C5-Testat. Wenn Ihre Organisation selbst Teil einer Lieferkette ist, zum Beispiel für KRITIS-Unternehmen oder die Verwaltung, sind auch Ihre eigenen Zertifizierungen und Testate von Bedeutung.
- **Einkauf:** Achten Sie verstärkt auf die Sicherheit bei der Beschaffung, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen. Dies beinhaltet auch die Behandlung und Offenlegung von Schwachstellen.
- **Effektivität:** Etablieren Sie Konzepte und Verfahren (KPIs, Audits, Penetrationstests etc.) zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit.
- **Training/Schulung und Sensibilisierung:** Schulen Sie Ihre Mitarbeitenden und stärken Sie die Awareness für Sicherheitsrisiken. Vermitteln Sie Best Practices für Cyberhygiene, um menschliche Fehler zu minimieren.
- **Sicherheitsmaßnahmen:** Um NIS2-Compliance zu erzielen, muss eine Reihe weiterer Maßnahmen umgesetzt werden. Dazu zählen neben Grundsätzen und Verfahren für den Einsatz von Kryptographie und gegebenenfalls Verschlüsselung auch die Personalsicherheit – also alle Maßnahmen, die IT-Sicherheitsrisiken durch den Faktor Mensch reduzieren. Ergänzend kommen Zugangskontrollmaßnahmen sowie Asset- und Risiko-Management (ISMS) hinzu. Die Nutzung von Multifaktor-Authentifizierungs- oder kontinuierlichen Authentifizierungslösungen, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung sollte ebenfalls sichergestellt sein.

Mit einem umfassenden Security-Portfolio, deutschen Cloud-Lösungen und einem breiten Partner-Ökosystem kann plusserver bei der Einhaltung gesetzlicher Vorgaben wie NIS2, aber auch SiG 2.0, unterstützen. Im Folgenden stellen wir einige der Lösungen im Kontext von NIS2 genauer vor.

Die Rolle eines Security Operations Centers (SOC) im Rahmen von NIS2-Compliance

Ein Security Operations Center (SOC) ist eine zentrale Einheit, die sich auf die Überwachung, Erkennung, Reaktion und Behebung von Sicherheitsvorfällen spezialisiert hat. Hier arbeiten Security-Analyst:innen mit einem Security Information and Event Management (SIEM), um Bedrohungen frühzeitig zu erkennen und angemessen zu reagieren. Die SIEM-Software bietet eine Echtzeitanalyse von Security-relevanten Meldungen aus den angebundenen Schnittstellen. Dies können Anwendungen oder auch Netzwerkkomponenten sein.

Welche Vorteile bietet ein Security Operations Center für NIS2-Compliance?

Durch die Kombination von Technologien, Prozessen und hochqualifizierten Fachleuten bietet ein SOC einen proaktiven Ansatz zur Sicherung kritischer Netzwerke und Systeme. Dieser Ansatz umfasst unter anderem:

Früherkennung von Sicherheitsvorfällen

Ein SOC überwacht kontinuierlich die Netzwerke und Systeme auf Anomalien und verdächtige Aktivitäten. Durch fortschrittliche Technologien wie IDS (Intrusion Detection System) und SIEM können potenzielle Sicherheitsvorfälle frühzeitig erkannt werden.

Incident Management

Im Falle eines Sicherheitsvorfalls ist eine schnelle Reaktion entscheidend. Das Incident Response Team im SOC unterstützt den Kunden dabei, Gegenmaßnahmen einzuleiten und die Auswirkungen zu minimieren. Dies trägt dazu bei, den Betriebsablauf aufrechtzuerhalten und den Schaden zu begrenzen.

Threat Intelligence

Ein SOC integriert aktuelle Threat Intelligence, um auf dem aktuellen Stand der Bedrohungslandschaft zu bleiben und Empfehlungen für präventive Maßnahmen zu geben.

Dokumentation und Compliance

NIS2 verlangt von Unternehmen eine umfassende Dokumentation ihrer Sicherheitsmaßnahmen und -vorfälle. Ein SOC erleichtert die Erfüllung dieser Anforderung, indem es detaillierte Protokolle und Berichte über Überwachungsaktivitäten und Incident-Response-Maßnahmen erstellt. Dies erleichtert die Einhaltung von Vorschriften und die Zusammenarbeit mit Regulierungsbehörden.

Welche Nachteile hat ein SOC?

So wertvoll ein SOC für ein hohes Security-Level ist, so aufwendig und kostspielig kann sich die Einrichtung und der Betrieb in Eigenregie gestalten. Auch die nötigen Fachkräfte sind rar gesät. Um von Skaleneffekten zu profitieren und die Einführung zu erleichtern, bietet sich daher die Nutzung eines SOC as a Service an. Ein Anbieter wie plusserver kümmert sich hierbei um die Infrastruktur und das Personal und stellt den Dienst zentral zur Verfügung.

Es besteht die Möglichkeit, zunächst einzelne Schnittstellen anzubinden, was die initialen Kosten und damit die Einstiegshürde noch weiter senkt. Dabei kann es sich auch um Security-Applikationen von Drittanbietern handeln, die bereits in der eigenen IT genutzt werden. Diese Logfiles können ebenfalls im SOC von plusserver ausgewertet werden.

Schwachstellenscans und weitere Maßnahmen

Einfach, aber wirkungsvoll ist die regelmäßige Überprüfung der IT-Landschaft auf mögliche Einfallstore für Cyberkriminelle. Dies unterstützt vor allem den Aspekt der frühzeitigen Detektion und Reaktion. Ein Vulnerability oder Security Scanner ist hier ein probates Mittel. Wie auch das SOC muss er nicht selbst angeschafft und betrieben werden, sondern die Scans lassen sich im gewünschten Umfang buchen.

So können IT-Verantwortliche durch die regelmäßige Durchführung von Schwachstellenscans eine umfassende Risikobewertung vornehmen. Dies ermöglicht es, priorisierte Maßnahmen zur Behebung von Sicherheitsproblemen zu ergreifen und Ressourcen effizient einzusetzen. Für die Erfüllung der Berichtspflichten gemäß NIS2 ist besonders interessant, dass Schwachstellenscanner auch Berichte generieren, welche die Ergebnisse von Sicherheitsscans zusammenfassen.

Was außerdem in den Security-Werkzeugkasten gehört, um den Anforderungen von NIS2 zu entsprechen:

- **Die Basis: Antivirus- und Antimalware-Lösungen.** Sie gehören auf jedes Endgerät und dienen dazu, Viren, Würmer, Trojaner und andere Arten von Malware zu erkennen und zu beseitigen.
- **Der Klassiker: Firewalls.** Sie gehören in jede IT-Infrastruktur und überwachen den Datenverkehr zwischen dem internen Netzwerk und externen Netzwerken. Sie können unautorisierten Zugriff blockieren und den Datenverkehr auf schädliche Aktivitäten überwachen. Einen Schritt weiter geht eine Next Generation Firewall. Sie bietet erweiterte Sicherheitsfunktionen, die über herkömmliche Firewalls hinausgehen, indem sie intelligente Bedrohungserkennung, Anwendungskontrolle und umfassendes Netzwerk-Monitoring kombiniert.
- **Der Türsteher: Intrusion Detection Systeme (IDS) und Intrusion Prevention Systeme (IPS).** Beide überwachen den Netzwerkverkehr auf verdächtige Aktivitäten. Ein IPS setzt aber nicht nur eine Alarmierung ab, sondern auch direkt die passenden Maßnahmen in Gang.
- **Das Schloss: Verschlüsselung** ist entscheidend, um sensible Daten während der Übertragung und im Ruhezustand zu schützen. Verantwortliche sollten sowohl Datenverschlüsselung als auch verschlüsselte Kommunikationsprotokolle in Betracht ziehen.

- **Der Kontrolleur: Authentifizierungstools** dienen der Multi-Faktor-Authentifizierung (MFA) und schaffen eine zusätzliche Security-Ebene. Starke Passwortrichtlinien sind wichtige Werkzeuge, um den Zugriff auf Systeme zu sichern.
- **Das Tagebuch: Log-Management** hilft bei der Sammlung, Analyse und Korrelation von Sicherheitsereignisprotokollen.
- **Das Pflaster: Effizientes Patch-Management** hält Software und Betriebssysteme auf dem neuesten Stand.
- **Die Verwaltung: Identity and Access Management (IAM)** dient der zentralen Verwaltung von Benutzeridentitäten und Zugriffsrechten. Indem nur autorisierte Personen auf kritische Systeme zugreifen, wird deren Verwundbarkeit drastisch reduziert.
- **Der Professor:** Last but not least gilt es, alle Mitarbeitenden für Security-Risiken zu sensibilisieren und ein sicherheitsbewusstes Verhalten zu fördern. Zu diesem Zweck können **Awareness-Tools,** aber auch persönliche Schulungen, eingesetzt werden.

NIS2 jetzt angehen!

Betroffene Organisationen müssen jetzt die erforderlichen Schritte unternehmen, um sicherzustellen, dass sie den Anforderungen dieser Richtlinie entsprechen. Sie benötigen Hilfe? Mit unserem breiten Partner-Ökosystem und umfangreichen Security-Portfolio begleiten wir Sie gern bei der Umsetzung der nötigen Maßnahmen.

› Sprechen Sie uns einfach an