ERSTE SCHRITTE MIT NIS2 – CHECKLISTE

Es wird erwartet, dass alle EU-Mitgliedstaaten bis 2024 NIS2 erfüllen. Dies bedeutet, dass spezifische Cyber-Security-Strategie befolgt, zuständige Behörden eingerichtet und Mechanismen zur Meldung von Vorfällen implementiert werden. NIS2 verlangt von den EU-Mitgliedsstaaten eine Zusammenarbeit beim Informationsaustausch, um sich vor Cyberangriffen zu schützen.

NIS2 baut auf den Anforderungen der ursprünglichen Richtlinie auf und zielt darauf ab, kritische Infrastrukturen und Organisationen in der EU vor Cyberbedrohungen zu schützen und ein hohes Maß an gemeinsamer Sicherheit in der gesamten EU zu erreichen.

Um dieses Ziel zu erreichen, verlangt NIS2 von den Mitgliedstaaten, eine Reihe zusätzlicher Maßnahmen zu ergreifen:

- Erstellung eines Vorfall-Reaktions-Plans, der mit Plänen anderer Mitgliedstaaten abgestimmt ist
- Aufbau eines nationalen “Computer Emergency Response Teams”
- Stärkung der Zusammenarbeit zwischen öffentlichen und privaten Stellen
- Verbesserung des Informationsaustauschs zwischen den Mitgliedstaaten

Hier finden Sie eine Checkliste, um sicherzustellen, dass die NIS2-Richtlinie eingehalten werden. Einfach durcharbeiten und die Punkte / Aufgaben abhaken. Erster Schritt: Gilt NIS2 für Sie? Ja, sicher!

Are you in one of these industries?

☐ Energie	☐ Bankwesen	☐ Luft- und Raumfahrt
☐ Regierung	☐ Finanzen	☐ Post/Kurier
☐ Andere öffentliche Verwaltung	☐ Herstellung	☐ Allgemeine Abfallwirtschaft
☐ Transport	☐ Wasser (Abfall/Trinken)	☐ Chemikalien (Entsorgung/Produktion)
☐ Polizei	☐ Digitale Infrastrukturen	☐ Wissenschaft
☐ Bildung	☐ Gesundheit & Pflege	☐ Nahrungsmittelindustrie

Die Einhaltung von NIS2 ist nicht optional. Dafür müssen Sie eine Reihe von Anforderungen erfüllen, aber alle Compliance-Anforderungen beginnen von Grund auf, bevor Sie überhaupt zu Sicherheitslösungen und -plattformen gelangen. Sie müssen sicherstellen, dass Ihre Kollegen im gesamten Unternehmen oder in der gesamten Organisation wissen, was von ihnen erwartet wird. Das hilft, um Risiken von Anfang an zu mindern.

Wichtiger Hinweis: Risikomanagement und -bewertungen sind ein laufender Prozess und erfordern konstantes Management. Sobald eine Risikobewertung durchgeführt wurde, ist es wichtig, regelmäßige Updates zu planen, um sicherzustellen, dass alle Schritte eingehalten werden.

Berücksichtigen Sie diese Punkte als Schritte. 1. Bewusstsein. 2. HR-Sicherheit. 3. Kontrolle von Assets – Wo sind sie, wie viele haben Sie, werden dieseaktualisiert? 4. Incident Management auf standardisierte und konsistente Weise. 5. Vulnerability Management - werden Ihre Systeme aktualisiert? 6. Bewertung des Risikos in Lieferketten. 7. Netzwerksicherheit. 8. Sicherheit in Entwicklungsprozessen – Wissen Sie, wer Ihren Code schreibt? 9. Zutrittskontrolle, sowohl physisch als auch virtuell. 10. Ggf. Einsatz von Verschlüsselung. 11. Notfallplanung - Was tun Sie, wenn jemand Ihr Netzwerk kompromittiert oder Ihre Daten stehlt oder Sie Ransomware erhalten?

JETZT GEHT'S LOS

Für Sie bedeutet das:

- [ ] Haben Sie die Anforderungen von NIS2 gelesen?
- [ ] Haben Sie ein umfassendes Verständnis für den entscheidenden Unterschied zwischen NIS und NIS2?
- [ ] Wissen Sie, wer für Compliance verantwortlich ist und wer haftbar gemacht wird, wenn Sie sich nicht daran halten?
  - [ ] Beachten Sie: Wissen Sie, dass Sie verantwortlich sind?

- [ ] Verfügt Ihre Infrastruktur über Funktionen zur Reaktion auf Vorfälle und zum Krisenmanagement?
- [ ] Bewerten Sie nun, wie Sie mit Schwachstellen und Offenlegung umgehen werden
  - [ ] Haben Sie eine Bewertung der damit verbundenen Risiken durchgeführt?

- [ ] Ist Ihre Lieferkette sicher?
  - [ ] Haben Sie die potenziellen Risiken für Ihre Lieferkette bewertet?
  - [ ] Haben Sie die mit Ihren Kunden verbundenen Risiken bewertet?

Damit Sie Ihren Kollegen helfen können:

- [ ] Verfügen Sie über Richtlinien und Verfahren zur Bewertung Ihrer Cybersicherheit?
- [ ] Haben Sie eine Cyber-Security-Schulung absolviert?
- [ ] Haben Sie Ihre Kollegen über die Bedeutung des Datenhandlings und der Compliance informiert?
- [ ] Haben Sie eine Reifegradbewertung durchgeführt?
- [ ] Haben Sie einen Plan für die weitere Strategie?

Computerhygiene

Es ist unerlässlich, die Mitarbeiter in Ihrem Unternehmen über die Notwendigkeit der Einhaltung der DSGVO und NIS2 zu informieren. Die Art und Weise, wie sie mit Daten auf Bodenebene umgehen, kann große Auswirkungen auf Daten und Compliance haben. Wenn Sie nicht wissen, wie Sie mit Daten und Informationen umgehen sollen, oder Daten entgegen der Einschätzung falsch gehandhabt werden, stellt dies ein kritisches Problem dar.

- [ ] Haben Sie Ihre grundlegenden Computerhygieneverfahren bewertet?
  - [ ] Reichen sie aus, um NIS2 zu erfüllen?
- [ ] Reichen sie aus, um NIS2 zu erfüllen?
  - [ ] Haben Sie eine Cyber-Security-Hygienerichtlinie?
  - [ ] Haben Sie diese im Unternehmen und sogar auf C-Level verteilt?
- [ ] Haben Sie eine zentrale Sicherheitsplattform?
  - [ ] Können Sie regelmäßige Aufgaben automatisieren?
- [ ] Haben Sie strenge Passwortrichtlinien für alle Mitarbeiter?
- [ ] Haben Sie sichergestellt, dass Sie eine ausreichende Multifaktor-Authentifizierung haben?
- [ ] Haben Sie einen Endpoint-Schutz?
- [ ] Haben Sie relevante Frameworks angewendet? NIST / ISO / CIS / Mitre Att&ck

Kryptographie

- [ ] Sind Sie sicher, dass sie Kryptographie denjenigen erklären können, die sie benötigen?
- [ ] Haben Sie Kryptografie effektiv angewendet?

Sonstiger Zeitpunkt

- [ ] Haben Sie konforme HR-Praktiken für Cyber Security?
- [ ] Haben Sie Richtlinien für HR-Sicherheitszugriff und -Kontrolle?
- [ ] Haben Sie Ihre Zugriffs- und Kontrollrichtlinien für die HR-Sicherheit einer Risikobewertung unterzogen?

Nichtbeachtung

- [ ] Sind Ihnen die Folgen einer Nichtbeachtung bekannt?

Was die richtige Cyber Security-Plattform tun kann, um sicherzustellen, dass Sie die Compliance einhalten

- [ ] Haben Sie ausreichende Maßnahmen zur Cyber Security?
  - [ ] SIEM
  - [ ] SOAR
  - [ ] UEBA
  - [ ] SAP System and Application Security
  - [ ] Endpoint security
  - [ ] Handelt es sich um eine SaaS-Lösung?
  - [ ] Handelt es sich um eine SaaS-Lösung mit Datensitz in der EU?

Berichterstellung

Berichte sind eine Anforderung von NIS2:

24 Stunden: Frühwarnung, die umfasst, wenn der Vorfall durch unrechtmäßige oder arglistige Handlungen verursacht wurde oder grenzüberschreitende Auswirkungen haben könnte.
72 Stunden: Benachrichtigung, die eine erste Bewertung mit Schweregrad und Auswirkungen sowie IOCs enthält.
Sofortige Berichte über Statusaktualisierungen, wie von der Behörde gefordert. Darüber hinaus: Ein abschließender Bericht spätestens einen Monat nach der ersten Benachrichtigung, der detaillierte Beschreibungen von Vorfällen, Arten von Bedrohungen, Minderungsmaßnahmen und grenzüberschreitende Auswirkungen von Vorfällen enthält.

- [ ] Stellt Ihnen Ihre Sicherheitsplattform Playbooks zur Verfügung, die automatisch Informationen sammeln, konvertieren und weitergeben, um die Meldeanforderungen zu erfüllen?

Incident Management

☐ NIS2 definiert die Handhabung von Vorfällen als: alle Aktionen und Verfahren, die darauf abzielen, einen Vorfall zu verhindern, zu erkennen, zu analysieren und zu begrenzen oder darauf zu reagieren und sich von einem Vorfall zu erholen.

☐ Haben Sie eine konsolidierte Lösung, die die Handhabung von Vorfällen erleichtert?

☐ Haben Sie die Sicherheit, SAP-Probleme/Sichtbarkeit in SAP-Systeme zur Überwachung und Handhabung von Vorfällen zu melden?

Weitere Zertifizierung und Konformität

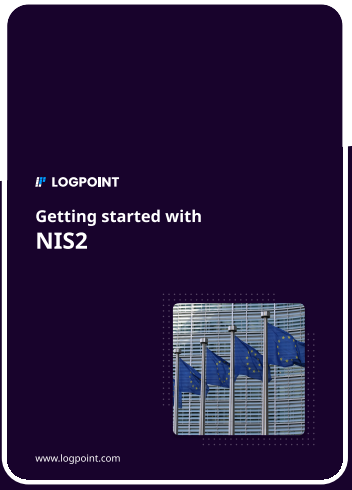
☐ Verfügt Ihre Sicherheit über die Common Criteria EAL3+ Zertifizierung?

☐ Entspricht sie der ISO 15408?

☐ Erfüllt Ihre Cybersicherheit Folgendes:

- ☐ DSGVO
- ☐ Schrems II
- ☐ CCPA

Mehr erfahren



ÜBER LOGPOINT

Logpoint ist der Entwickler einer zuverlässigen, innovativen Cybersecurity-plattform, die Unternehmen weltweit in die Lage versetzt, in einer Welt voll stetig entwickelnder Bedrohungen, erfolgreich zu sein.
Durch die Kombination aus ausgeklügelter Technologie und einem tiefgreifenden Verständnis der Kundenherausforderungen stärkt Logpoint die Fähigkeiten der Sicherheitsteams und hilft ihnen, aktuelle und zukünftige Bedrohungen zu bekämpfen. Logpoint bietet SIEM-, UEBA- und SOAR-Technologien in einer einheitlichen, vollständigen Plattform, die Bedrohungen effizient erkennt, False Positives minimiert, Risiken eigenständig priorisiert, auf Vorfälle reagiert und vieles mehr. Logpoint hat seinen Hauptsitz in Kopenhagen (Dänemark) und ist ein multinationales, multikulturelles und integratives Unternehmen mit Niederlassungen auf der ganzen Welt.