Wie Eye Security unterstützen kann

NIS2 in der Praxis: Compliance-Bereitschaft gezielt stärken.

Viele Pflichten unter NIS2, etwa Governance-Entscheidungen, Risikoverantwortung und Rechenschaftspflichten, verbleiben fest bei der Organisation und ihrem Management. Diese Aufgaben können nicht an externe Anbieter übertragen werden.

Eine zentrale operative Anforderung nach NIS2 ist die Fähigkeit, Sicherheitsvorfälle zu erkennen und darauf zu reagieren. Organisationen müssen ihre Umgebungen kontinuierlich überwachen, Bedrohungen frühzeitig identifizieren und schnell handeln, um Vorfälle einzudämmen. Eye Security unterstützt genau diese Anforderungen durch 24/7 SOC-Monitoring und Incident Response. Wir helfen Ihnen, Vorfälle zu untersuchen, einzudämmen und zu beheben und gleichzeitig die Meldepflichten einzuhalten. Dabei unterstützen wir Sie bei der Umsetzung, Operationalisierung und Nachweisführung der zentralen NIS2-Anforderungen in den Bereichen Erkennung und Reaktion.

Die nachfolgende Übersicht zeigt Ihre Pflichten nach NIS2 und macht deutlich, wo Eye Security direkte Unterstützung, Tools oder fachlichen Rat bieten kann, während Governance, finale Entscheidungen und rechtliche Verantwortung bei Ihnen verbleiben.

> Für Führungskräfte im Bereich Cybersecurity bedeutet „Assume Breach" einen Paradigmenwechsel: weg von punktueller Compliance, hin zu kontinuierlicher Einsatzbereitschaft. Organisationen müssen Reaktionspläne regelmäßig testen, Teams gezielt schulen, Systeme rund um die Uhr überwachen und externe Expertise einbinden.
>
> **Marcel van Asperdt**
> CISO, Eye Security

↘ Die hervorgehobenen Bereiche zeigen, wo Eye Security direkte Unterstützung bietet oder die Umsetzung über zertifizierte Partner ermöglicht. Die endgültige Verantwortung für Compliance, Berichterstattung und Nachbesserungen bleibt stets beim Unternehmen, auch wenn Eye Security die operative Umsetzung unterstützt.

Governance und Verantwortlichkeiten

- ✓ Verantwortliche Person oder Team für NIS2-Compliance benennen
- ✓ Cybersicherheitsrichtlinien vom Vorstand genehmigen lassen
- ✓ Management zu NIS2-Pflichten schulen
- ✓ Rollen und Zuständigkeiten für Incident Response dokumentieren

Risikomanagement

- ✓ Regelmäßige Risikobewertungen für IT- und OT-Systeme durchführen
- ✓ Informationssicherheitsrichtlinie nach ISO 27001 oder NIST pflegen
- ✓ Inventar und Klassifizierung von IT-Assets erstellen
- ✓ Sensible Daten verschlüsseln

Technische und organisatorische Maßnahmen

- Zugriffskontrollen mit Multi-Faktor-Authentifizierung
- Prozess für Patch- und Schwachstellenmanagement implementieren
- Sichere Beschaffung, Entwicklung und Wartung von Systemen
- Netzwerksegmentierung und Firewall-Regeln umsetzen
- Sichere Kommunikation gewährleisten (TLS, VPN)

Geschäftskontinuität

- Notfall- und Wiederherstellungspläne erstellen und testen
- Backup-Strategie pflegen (offline und unveränderbare Backups)
- Recovery Time Objectives (RTO) und Recovery Point Objectives (RPO) definieren

Dokumentation und Nachweisführung

- Audit-Logs für sicherheitsrelevante Ereignisse bereitstellen
- Aufzeichnungen zu Compliance-Aktivitäten führen
- Vorbereitung auf Audits und behördliche Prüfungen

Incident-Management

- Incident-Response-Plan entwickeln und regelmäßig testen
- Unterstützung bei der Erstellung von Berichten
  - Frühwarnung innerhalb von 24 Stunden
  - Detaillierter Bericht innerhalb von 72 Stunden
- Kontakt zu nationalen CSIRTs aufbauen

Lieferketten-Sicherheit

- Risiken von Drittanbietern für kritische Lieferanten bewerten
- Cybersecurity-Klauseln in Lieferantenverträge aufnehmen
- Sicherheitsstatus von Dienstleistern kontinuierlich überwachen

Schulung und Sensibilisierung

- Regelmäßige Cybersecurity-Schulungen für Mitarbeitende durchführen
- Phishing-Simulationen und Awareness-Kampagnen umsetzen

Governance-Reporting

- Jährliche Compliance-Reviews planen
- Berichterstattung an Management und Aufsichtsbehörden gemäß Anforderungen

Über Eye Security

Eye Security unterstützt kleine und mittelständische Unternehmen dabei, Cyberrisiken proaktiv zu erkennen und die operative Resilienz zu stärken. Als führender europäischer MDR-Anbieter vereint Eye Security modernste KI-Technologie, umfassende Expertise und nahtlos integrierte Cyberversicherung. Über 800 europäische Kunden setzen auf die ganzheitliche Schutzlösung, um ihre digitalen Prozesse zuverlässig zu schützen.

www.eyesecurity.de

Incident-Response-Hotline

Cybervorfall? Rufen Sie die Eye Security Incident-Response-Hotline rund um die Uhr unter **+49 (0)203 6688 1900** an. Für nicht dringende Fälle erreichen Sie das IRTeam per E-Mail unter **cert@eye.security**.