NIS2 Incident Response Starter Kit.

Ein Leitfaden zur Vorbereitung auf die 24- und 72-Stunden-Meldepflicht

Im Rahmen von NIS2 müssen Organisationen in der Lage sein, erhebliche Cybervorfälle schnell und strukturiert zu erkennen und zu melden. In der Praxis fehlen häufig nur wenige, aber entscheidende Bausteine: klare Verantwortlichkeiten, ein getesteter Reaktionsprozess und die Fähigkeit, unter Zeitdruck die richtigen Informationen zusammenzutragen.

Dieses Starter Kit beschreibt einen Mindestansatz für Incident-Response-Readiness. Ziel ist es, den Geschäftsbetrieb zu schützen, die NIS2-Meldepflichten innerhalb von 24 und 72 Stunden zu erfüllen und den Schaden im Ernstfall zu begrenzen.

Was NIS2 von Ihnen erwartet

NIS2 verlangt von Organisationen den Nachweis, dass sie in der Lage sind:

- ✓ Cybervorfälle zu erkennen und darauf zu reagieren
- ✓ Vorfälle als Geschäftsrisiko zu managen, nicht nur als technisches Problem
- ✓ Innerhalb von 24 Stunden eine Frühwarnmeldung abzugeben
- ✓ Innerhalb von 72 Stunden eine Folgemeldung mit Fakten und einer Bewertung der Auswirkungen einzureichen
- ✓ Technische, rechtliche und geschäftliche Entscheidungen während eines Vorfalls koordiniert zu treffen

Ihr 3-Schritte-Plan

Schritt 1

Klare Verantwortlichkeiten festlegen

Klare Zuständigkeiten verhindern Verzögerungen und Unsicherheiten in den ersten, entscheidenden Stunden. Definieren Sie vor einem Vorfall verbindlich, wer verantwortlich ist für:

- Gesamtleitung und Koordination des Vorfalls
- Technische Analyse und Eindämmung
- Geschäfts- und Risikobewertungen
- Interne und externe Kommunikation
- Regulatorische Meldungen und Dokumentation

Schritt 2

Einen schlanken Incident-Response-Plan erstellen

Ein wirksamer Incident-Response-Plan muss nicht umfangreich sein. Wir empfehlen einen kompakten, auch in gedruckter Form verfügbaren Plan, der mindestens folgende Punkte abdeckt:

- Wie Vorfälle erkannt und eskaliert werden
- Wer entscheidet, ob ein Vorfall als erheblich einzustufen ist
- Welche Rollen und Verantwortlichkeiten im Ernstfall greifen
- Wie Eindämmung und Untersuchung eingeleitet werden
- Wie Beweise und Protokolldaten gesichert werden
- Wie Informationen für die 24- und 72-Stunden-Meldung strukturiert gesammelt werden

Schritt 3

Eine Tabletop-Übung durchführen

Eine einzige Tabletop-Übung liefert häufig mehr Erkenntnisse als monatelange Planung. Wählen Sie ein plausibles Szenario, etwa einen Ransomware-Vorfall, und prüfen Sie gemeinsam:

- Wer wird informiert und wie schnell
- Wer trifft in den ersten Stunden welche Entscheidungen
- Welche Maßnahmen in den ersten vier Stunden eingeleitet werden
- Welche Informationen nach 24 Stunden tatsächlich vorliegen würden
- Wo Lücken für die 72-Stunden-Meldung bestehen

Wenn Sie nur fünf Dinge umsetzen …

Bereits die folgenden fünf Maßnahmen reduzieren Melderisiken und operative Unsicherheit deutlich:

1. Benennen Sie eine Incident-Leitung sowie eine Stellvertretung.
2. Legen Sie intern fest, was als erheblicher Vorfall gilt.
3. Erstellen Sie eine Checkliste für die 24-Stunden-Meldung mit den erforderlichen Fakten.
4. Stellen Sie sicher, dass Protokolldaten und Identitätsaktivitäten zentral erfasst und zugänglich sind.
5. Testen Sie noch in diesem Monat ein realistisches Szenario.

Typische Lücken in der Praxis

In unserer täglichen Arbeit sehen wir wiederkehrende Schwachstellen:

- Keine klar benannte verantwortliche Person in den ersten Stunden
- Incident-Response-Pläne, die nie praktisch getestet wurden
- Technische Teams konzentrieren sich auf Wiederherstellung, während meldepflichtige Informationen fehlen
- Beweismittel werden überschrieben oder sind bei regulatorischen Rückfragen nicht verfügbar
- Geschäftsführung und Vorstand sind unsicher, welche Entscheidungen wann erforderlich sind

Wie Eye Security Sie bei der NIS2-Readiness unterstützt

Eye Security unterstützt Organisationen in ganz Europa mit praxisnaher Incident Response und kontinuierlicher Erkennung von Bedrohungen. Dazu gehören:

- 24/7 Detection and Response über unser europäisches Security Operations Centre (SOC)
- Praxisorientierte Incident-Response-Planung im Einklang mit den Anforderungen von NIS2
- Konkrete Vorbereitung auf die 24- und 72-Stunden-Meldung mit klarer Definition, welche Informationen wann und aus welchen Quellen erhoben werden müssen
- Hands-on-Unterstützung bei Untersuchung und Eindämmung der Vorfälle
- Stärkung grundlegender Sicherheitskontrollen zur Reduzierung von Auswirkungen, Ausfallzeiten und Meldeaufwand

Gerne sprechen wir mit Ihnen über Ihre Incident-Response-Planung und eine kontinuierliche 24/7-Überwachung.

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 IR-Team per E-Mail unter **cert@eye.security**.