RAPID7

DIE 24-STUNDEN-REGEL VON NIS2: BEREITSCHAFT HAT EINE UHR

NIS2 macht die Meldung von Incidents zu einer zeitlich begrenzten operativen Verpflichtung. Bei schwerwiegenden Incidents müssen die Unternehmen unter Umständen innerhalb von 24 Stunden nach Bekanntwerden des Vorfalls eine Frühwarnung herausgeben. Das macht die Reportingbereitschaft zu mehr als einer Grundsatzfrage. Sie wird zum Prüfstein dafür, wie effektiv Erkennung, Eskalation, Koordination und Governance auch unter hohem Zeitdruck funktionieren.

STUNDE 0

Bewusstsein setzt die Uhr in Gang

Die erste Herausforderung besteht darin, zu erkennen, wann ein schwerwiegender Incident eine Benachrichtigung auslösen könnte. Die 24-Stunden-Frist beginnt mit dem Zeitpunkt der Kenntnisnahme, nicht erst mit dem Abschluss der Untersuchung.

STUNDEN 1-4

Bewertung und Eskalation

Teams müssen schnell erkennen, bewerten und eskalieren. Das bedeutet, zu verstehen, was passiert ist, wer beteiligt sein muss und ob der Incident die Meldeschwelle erreichen kann.

STUNDEN 4-12

Erstellen des Incident-Bildes

Ein vollständiges forensisches Bild ist am ersten Tag nicht erforderlich. Aber Organisationen benötigen genügend Kontext, um die Bedeutung zu verstehen, die Entscheidungsfindung zu unterstützen und mit der Vorbereitung einer Frühwarnung zu beginnen.

12-24 UHR

Vorbereiten der Frühwarnung

Bei der Frühwarnung geht es um rechtzeitige Benachrichtigung, nicht um absolute Gewissheit. Organisationen benötigen ausreichende Koordination, Governance-Bereitschaft und belastbare Nachweise, um unverzüglich handeln zu können.

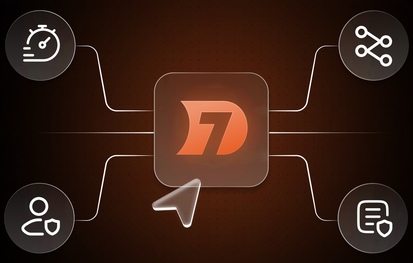
WAS TEAMS HÄUFIG VERLANGSAMT

Manuelle Workflows, fragmentierte Sichtbarkeit, unklare Zuständigkeiten und schwache Eskalationspfade können die Erfüllung der 24-Stunden-Anforderung erschweren.

SO SIEHT EINE WIRKSAME VORBEREITUNG AUS

Eine hohe Meldebereitschaft basiert auf:

- ☑ Der schnellen Erkennung und Bewertung von Sicherheitsvorfällen
- ☑ Klar definierten Eskalationswegen
- ☑ Einer nachvollziehbaren Dokumentation von Vorfällen und Zeitabläufen
- ☑ Einer wirksamen Aufsicht durch die Unternehmensleitung



Die 24-Stunden-Frühwarnung ist nur die erste Stufe. NIS2 sieht auch eine umfassendere Meldung des Incidents innerhalb von 72 Stunden und einen Abschlussbericht innerhalb eines Monats vor.

24 STUNDEN → 72 STUNDEN → 1 MONAT

DRUCK IN HANDLUNGSFÄHIGKEIT VERWANDELN

Rapid7 unterstützt Unternehmen dabei, ihre Meldebereitschaft zu stärken, indem die ersten 24 Stunden eines Sicherheitsvorfalls in der Praxis leichter zu bewältigen sind. InsightIDR und der Insight Agent helfen Teams dabei, die für die Erkennung verdächtiger Aktivitäten erforderlichen Protokoll-, Endpunkt- und Asset-Daten zu erfassen und miteinander zu verknüpfen. So entsteht bereits frühzeitig ein klareres Bild des Vorfalls. Managed Detection and Response ergänzt dies durch die Expertise erfahrener Analysten. Sie unterstützen dabei, die Schwere eines Vorfalls einzuschätzen, Untersuchungen auf die relevantesten Risiken zu fokussieren und fundierte Entscheidungen unter Zeitdruck zu treffen. Digital Forensics und Incident Response hilft Teams dabei, die erforderlichen Beweise zu sichern und auszuwerten, um nachvollziehen zu können, was passiert ist, wann der Vorfall erkannt wurde und wie darauf reagiert wurde. Gemeinsam tragen diese Fähigkeiten dazu bei, eine belastbare Nachweisgrundlage für die frühzeitige Meldung und die Reaktion auf Sicherheitsvorfälle zu schaffen – während die Verantwortung dort bleibt, wo sie hingehört: beim Unternehmen selbst.

RAPID7