

Security Awareness in der **NIS-2-Richtlinie**

Dr. Christian Reinhardt



| Oktober 2024



SOSAFE

Europas größter Anbieter für Security Awareness und Human Risk Management



>500

Mitarbeitende mit vielfältigen Backgrounds

>3.5M

users worldwide

>5,000

customers across all industries



>32

Badges



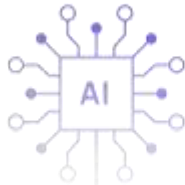
ERHÖHTES CYBERRISIKO

... dahinter stehen drei große Antriebsfaktoren

Neue Technologien



der Security-Verantwortlichen halten den Einsatz generativer KI durch Cyberkriminelle für besorgniserregend, bei Unternehmen mit mehr als 5.000 Mitarbeitern sind es sogar 86 %.



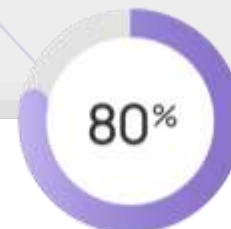
Globale Instabilität



3 von 4 Security-Verantwortliche bestätigen, dass die geopolitische Lage das Sicherheitsrisiko ihrer Organisation erhöht hat.



Vernetzung



der Security-Verantwortlichen erkennen zunehmend die Bedeutung der Lieferkettensicherheit.



Quelle: Human Risk Review, 2024

VERDICT

The state of cybersecurity: AI and geopolitics mean a bigger threat than ever

Cyber
MAGAZINE

Artikel • Heftung 5/2024
HP: Businesses Fear Physical Supply Chains Pose Cyber Risk

Was sind die Ziele der NIS2-Richtlinie?

- **Implementierung von Asset-Management-Verfahren**
- Beseitigung von Inkonsistenzen und Optimierung der Kommunikation und Zusammenarbeit
- **Meldung von Vorfällen bei den zuständigen Stellen** und Gewährleistung der effizienten Reaktion auf Zwischenfälle
- Definition und Umsetzung von **Cybersicherheitsstrategien**
- **Ausarbeitung von Protokollen, Vorgaben und Reaktionsplänen**
- Umsetzung von **Sicherheitsmaßnahmen für die Lieferkette**, um die Sicherheit externer Anbieter zu überprüfen und zu gewährleisten
- Entwicklung einer Strategie für die Gewährleistung der **durchgängigen Bereitstellung kritischer Dienste** bei Sicherheitsvorfällen
- **Bereitstellung von Training und Steigerung des Bewusstseins der Mitarbeitenden** und Wahrung der schnellen Reaktionsfähigkeit

Der Faktor Mensch wird in den Anforderungen der NIS2 berücksichtigt

Kapitel 1 - Artikel 11, §3(d) „Die CSIRTs haben folgende Aufgaben...dynamische Analyse von Risiken und Sicherheitsvorfällen sowie Lagebeurteilung im Hinblick auf die Cybersicherheit“

Kapitel 4 - Artikel 20, §2 & Artikel 21, §2(g) „Mitgliedstaaten stellen sicher, dass die Mitglieder der Leitungsorgane wesentlicher und wichtiger Einrichtungen an Schulungen teilnehmen müssen, und fordern wesentliche und wichtige Einrichtungen auf, allen Mitarbeitern regelmäßig entsprechende Schulungen anzubieten“ ...über...„grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit“



Präambel (89) „Die wesentlichen und wichtigen Einrichtungen sollten eine breite Palette grundlegender Praktiken der Cyberhygiene anwenden, z. B. Zero-Trust-Grundsätze, Software-Updates, Gerätekonfiguration, Netzwerksegmentierung, Identitäts- und Zugriffsmanagement oder Sensibilisierung der Nutzer, Schulungen für ihre Mitarbeiter organisieren und das Bewusstsein für Cyberbedrohungen, Phishing oder Social-Engineering-Techniken schärfen.“

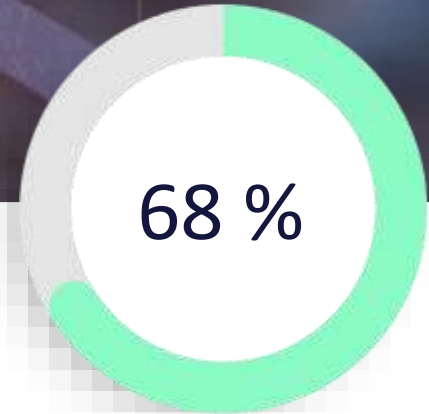
Präambel (78) „Die Risikomanagementmaßnahmen im Bereich der Cybersicherheit sollten eine systemische Analyse vorsehen, bei der der menschliche Faktor berücksichtigt wird, um ein vollständiges Bild der Sicherheit des Netz- und Informationssystems zu erhalten.“

FAKT IST:

**Cyberkriminelle
konzentrieren ihre
Angriffe auf ein
Hauptziel**



Menschen



der Sicherheitsverstöße sind auf ein **nicht böswilliges menschliches Element** zurückzuführen, z. B. eine Person, die sich von einem Social-Engineering-Angriff täuschen lässt oder einen Fehler begeht.

Quelle: Verizon, 2024

Womit anfangen?

Awareness

1. Großer Impact

2. Kleiner Aufwand





Klingt spannend?

Lassen Sie uns diskutieren!

Dr. Christian Reinhardt

Awareness Evangelist

SoSafe

christian.reinhardt@sosafe.de

LinkedIn

