Schutz wichtiger Infrastruktur
unter Einhaltung der gesetzlichen Anforderungen

Weltweit gibt es immer mehr schädliche Angreifer, die versuchen, das öffentliche Leben und die Sicherheit massiv zu stören, indem sie mit Cyberangriffen auf kritische Infrastrukturen zielen.

Was ist NIS2?

- neue EU-weite Gesetzgebung zur Verbesserung der Cybersicherheit
- Resilienz und die Reaktion auf Sicherheitsvorfälle des öffentlichen und des privaten Sektors steigern
- strikte Kontrollmaßnahmen
- Stärkung der Meldepflicht-Anforderungen
- bis zum 17. Oktober 2024 Umsetzung ins nationales Recht der Mitgliedsstaaten

Wer ist betroffen?

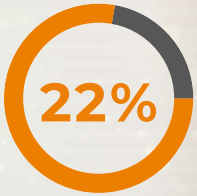
Betroffen sind **große und mittlere** Unternehmen aus folgenden Sektoren:

Weltweit steigen die Cyber-Angriffe auf sensible Strukturen kontinuierlich an.

Cyberangriffe auf kritische Infrastrukturen weltweit - ein Anstieg um 20 % seit Juni 2020.

Organisationen mit kritischen Infrastrukturen, die keine Zero-Trust-Strategien anwenden.

Energie-, Öl- und Gasindustrie sowie das verarbeitende Gewerbe waren von Cyberangriffen betroffen. Dies hatte Auswirkungen auf die Produktion und die Energieversorgung.



Anstieg der DDoS-Angriffe auf Finanzunternehmen weltweit im Vergleich zum Vorjahr

Durchschnittliche Kosten für Datenschutzverletzungen im Gesundheitswesen - der höchste Wert im Vergleich zu anderen Branchen.

Sources
Microsoft, Government Technology, IBM, Trend Micro, FS-ISAC

Vorgeschriebene Maßnahmen

- Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme
- Bewältigung von Sicherheitsvorfällen
- Aufrechterhaltung des Betriebs nach einem Notfall, und Krisenmanagement
- Sicherheit der Lieferkette
- Sicherheitsmaßnahmen bei Erwerb/Entwicklung/Wartung von IKT
- Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagement-maßnahmen
- Cyberhygiene und Schulungen zur Cybersicherheit
- Kryptografie und ggf. Verschlüsselung
- Sicherheit des Personals, Konzepte für die Zugriffskontrolle

MULTI-FAKTOR-AUTHENTIFIZIERUNG (MFA)

yubico

Phishing-resistenten MFA
zur Sicherung kritischer Infrastrukturen

Ein zentraler Bestandteil der Cybersicherheitsstrategie der Europäische Union ist die Multifaktor-Authentifizierung (MFA). So ist laut Artikel 21 2. j) ist die Verwendung von Lösungen für die mehrstufige Authentifizierung oder die kontinuierliche Authentifizierung innerhalb der Einrichtung verpflichtend. Jeodoch ist nicht alle Formen der MFA sind gleich. Moderne phishingresistente Authentifizierung und hardwaregestützte Sicherheit sind der beste Weg, um die kritischsten Informationen, Prozesse und IT- und OT-Systeme zu schützen, auf die sich unsere Wirtschaft stützt.
Deshalb ist diese Methode zum Standard für Regierungsbehörden und eine wachsende Zahl von Regulierungsbehörden geworden.

Integration

in neue und bereits bestehende Infrastrukturen

Yubico bietet mit dem YubiKey eine umfassende Lösung zur Stärkung der Cyber-Resilienz von Unternehmen. Dieses Hardware-Sicherheitstoken unterstützt sowohl PIV als auch FIDO2 und kann den passwortbasierten Authentifizierungsfluss durch eine phishingsichere Alternative ersetzen. Mit verschiedenen Formfaktoren, darunter auch FIPS und CSPN zertifizierte Keys für den besonders streng regulierten Bereich, bietet Yubico skalierbare Optionen für Unternehmen aller Größen. Der YubiHSM ergänzt das Angebot als kosteneffiziente Toolbox für die sichere Speicherung und Generierung von kryptografischem Material.

Trotz vermeintlicher Komplexität der NIS2-Richtlinie, sind die Grundlagen der Sicherheit bei näheren Betrachtung jedoch einfach. Jede Investition in die Cyber-Resilienz, die über die reine NIS2-Erfüllung hinausgeht, ist lohnenswert um zukünfige Angriffe zu vermeiden.

sysob und Yubico steht bereit, Unternehmen bei der Bewältigung der Cybersicherheits-herausforderungen zu unterstützen.

Ihr Yubico Ansprechpartner by sysob
Markus Senbert / Channel Sales Directo / msenbert@sysob.com

[sysob]:::