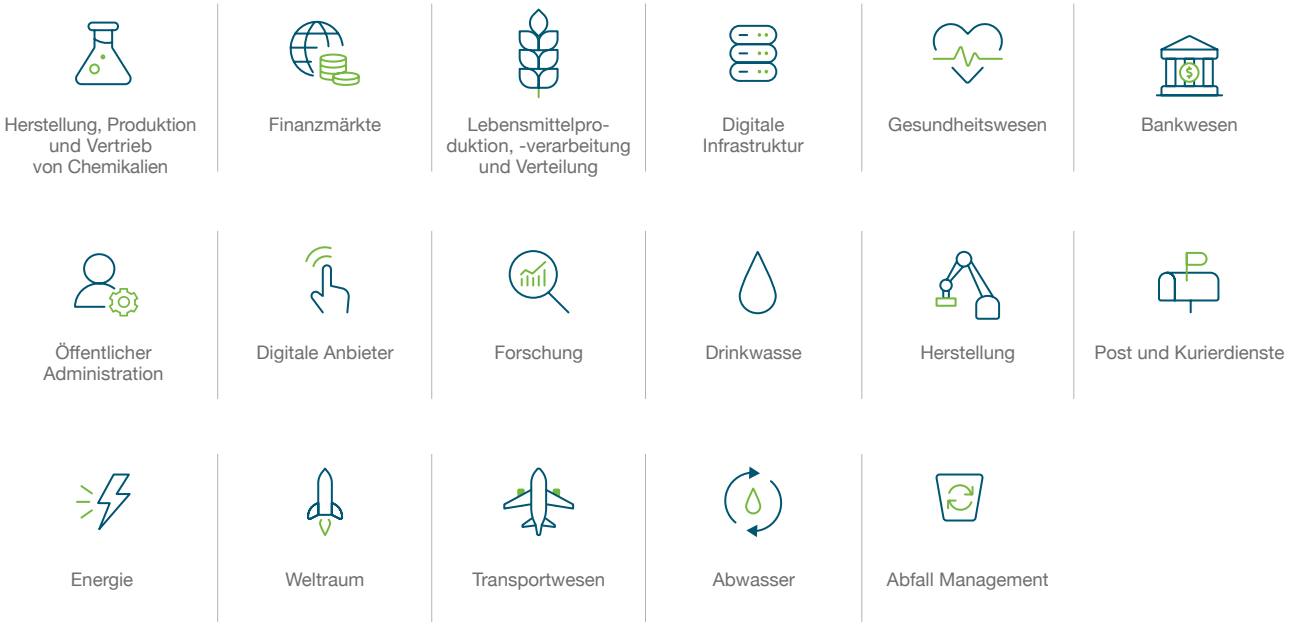
Liebe CEOs: Die Sicherheit einer systemkritischen Infrastruktur beginnt bei Ihnen – und hängt von einer Phishing-resistenten MFA ab

Eine wachsende Anzahl von Cyberkriminellen versucht, die öffentliche Sicherheit zu stören, indem sie systemkritische Infrastrukturen anvisieren. Als Führungskraft einer Organisation mit systemkritischer Infrastruktur ist es Ihre Aufgabe, eine Kultur der Cybersicherheit zu schaffen.

Wird Ihr Unternehmen als systemkritisch angesehen?

Die Definitionen, was genau unter systemkritischer Infrastruktur zu verstehen ist, variieren je nach Land, doch ein Merkmal haben sie alle gemeinsam: Sektoren, in denen eine Beeinträchtigung oder Zerstörung die Sicherheit eines Landes, die wirtschaftliche Sicherheit, die öffentliche Gesundheit und/oder die Sicherheit beeinträchtigen würde und die eine physische Bedrohung für Menschenleben darstellen können. Die NIS2-Richtlinie definiert wesentliche und wichtige Einrichtungen in diesen Branchen:

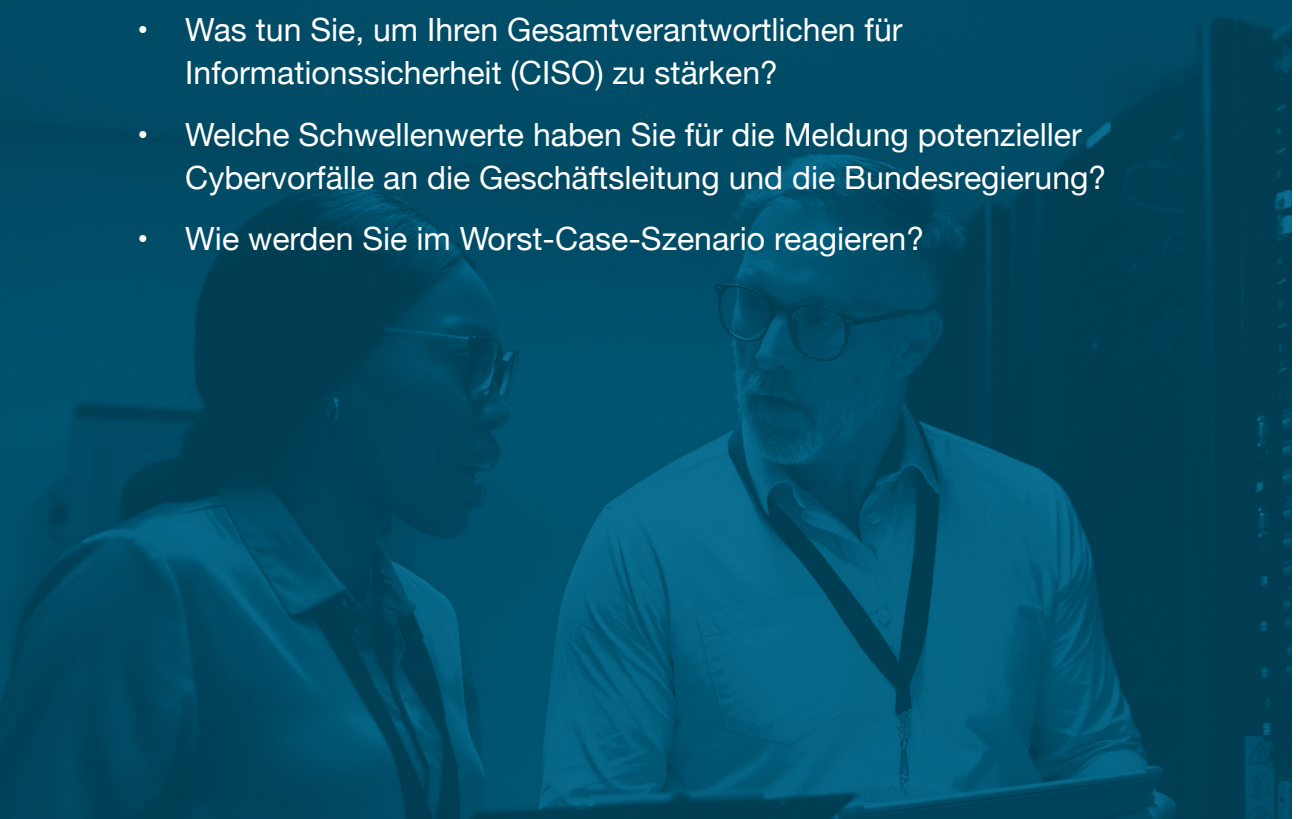


Was sind Kritische Infrastrukturen? (BSI)

yubico

Nur 51 % der CEOs verlangen Pläne für das Cyberrisikomanagement bei größeren geschäftlichen oder betrieblichen Veränderungen. Fragen Sie sich also Folgendes:

- Wissen Ihre Führungskräfte, wie sie auf einen Cybervorfall reagieren müssten?
- Welche Pläne hat Ihr Unternehmen, um die Geschäftskontinuität aufrechtzuerhalten?
- Was tun Sie, um Ihren Gesamtverantwortlichen für Informationssicherheit (CISO) zu stärken?
- Welche Schwellenwerte haben Sie für die Meldung potenzieller Cybervorfälle an die Geschäftsleitung und die Bundesregierung?
- Wie werden Sie im Worst-Case-Szenario reagieren?



Der unwiderlegbare Beweis, dass Cyberbedrohungen, die sich auf kritische Infrastrukturen richten, nur allzu real sind:

40 %

Cyberangriffe auf kritische Infrastruktur weltweit **sind von 20 %** aller Angriffe von Nationen **auf 40 % gestiegen** (Quelle)

25 %

Lagebericht Cybercrime 2023 - BSI: Die Anzahl der eingehenden Meldungen zu Cyberangriffen auf kritische Infrastrukturen stieg im Jahr 2023 um **25 %** im Vergleich zum Vorjahr (Quelle)

80 %

Fast 80 % der kritischen Infrastrukturunternehmen, die in einem IBM-Bericht aus dem Jahr 2022 untersucht wurden, haben keine Zero-Trust-Strategien eingeführt. Dadurch stiegen die durchschnittlichen Kosten für Sicherheitsverletzungen auf 5,4 Millionen USD – 1,17 Millionen USD mehr im Vergleich zu Unternehmen, die Strategien hatten (Quelle)

$9,23 Millionen

Das Gesundheitswesen verursacht mit **9,23 Millionen USD** die höchsten durchschnittlichen Gesamtkosten für eine Datenschutzverletzung (Quelle)

89 %

89 % der Unternehmen in den Bereichen Strom, Öl und Gas sowie in der Fertigung waren zwischen Mitte 2021 und Mitte 2022 von Cyberangriffen betroffen, die sich auf die Produktion und Energieversorgung auswirkten (Quelle)

yubico

Jeder CEO sollte seine Geschäfts-kontinuitätsstrategie mit einer Phishing-resistenten MFA beginnen

Ein wichtiger Bestandteil einer erfolgreichen Cybersicherheitsstrategie sind eine Multi-Faktor-Authentifizierung (MFA) und gerätegebundene Passkeys, **doch nicht alle Formen der MFA sind gleich.** Moderne, Phishing-resistente Authentifizierung und hardwarebasierte Sicherheit bieten die beste Möglichkeit, die wichtigsten Informationen, Prozesse sowie IT- und OT-Systeme zu schützen, auf die unsere Gesellschaft angewiesen ist. Deshalb ist sie zum Standard für Behörden und eine wachsende Anzahl von Aufsichtsbehörden geworden.

Um mehr darüber zu erfahren, wie echte Unternehmen systemkritischer Branchen diese innerhalb Ihrer Betriebe, Lieferketten und weltweit umsetzen, besuchen Sie:

Ein US-Bundesstaat nutzt den YubiKey, um die Wählerregistrierungsdatenbanken vor Hackern zu schützen

LESEN SIE DIE FALLSTUDIE

yubi.co/USGovernment

Schneider Electric erhöht die Sicherheit der globalen Lieferkette mit YubiKeys und YubiHSM

LESEN SIE DIE FALLSTUDIE

yubi.co/SchneiderElectric

YubiKeys verteidigen das nationale Öl- und Gasunternehmen der Ukraine vor Cyberangriffen

LESEN SIE DIE FALLSTUDIE

yubi.co/Naftogaz

yubico

In einer durch und durch vernetzten Welt ist jeder Einzelne für die Stärkung des Cybersicherheits-Ökosystems verantwortlich

„Eine der größten Cybersicherheitsbedrohungen ist der menschliche Faktor, etwa, wenn Cyberkriminelle durch Phishing-Angriffe an Passwörter oder Zugangsdaten gelangen.“

Oleksandr Tarasov

Leiter der Sicherheitskontrollen im Security Operation Center, Naftogaz-Bezreka (nationales Öl- und Gasunternehmen der Ukraine)

Yubi.co/Naftogaz

10 %

10 % aller Datenschutzverletzungen betreffen Finanzdienstleistungen (Quelle)

11 Staaten

11 US-Bundesstaaten erlitten im Rahmen des Ransomware-Angriffs auf Colonial Pipeline im Jahr 2021 vorübergehende Gasausfälle (Quelle)

Die Anzahl der Cybersicherheitsvorfälle, die die kritische Infrastruktur Australiens betrafen, stieg im Geschäftsjahr 2022/23 um fast ein Drittel (Quelle)

Cyberkriminelle haben die polnische Börse lahmgelegt (Quelle)

Japan hat in den letzten Jahren einen Anstieg von Cyberangriffen auf seine kritische Infrastruktur, Industrie und Regierungsbehörden erlebt (Quelle)

Yubico (Nasdaq First North Growth Market Stockholm: YUBICO) ist Erfinder des YubiKey, dem Goldstandard für eine Phishing-resistente Multi-Faktor-Authentifizierung (MFA), und hat wesentlich zur Entwicklung der offenen FIDO-Authentifizierungsstandards beigetragen. Das Unternehmen ist ein Pionier bei der Bereitstellung einer hardwarebasierten Passkey-Authentifizierung für Kunden in über 160 Ländern. Weitere Informationen finden Sie unter: www.yubico.com.

Kontaktieren Sie uns
yubi.co/kontakt

yubico