swissbit®

White Paper

Multifaktor-Authentifizierung: NIS2-Anforderungen erfüllen, Haftungsrisiken vermeiden

swissbit®

Die NIS2-Richtlinie der Europäischen Union schreibt Zugriffskontrollen zum Schutz kritischer Infrastrukturen und wesentlicher Dienste vor. Viele Unternehmen, Behörden andere Organisationen sind davon betroffen und müssen rechtzeitig handeln, um empfindliche Strafen bis hin zur persönlichen Haftung zu vermeiden. Wie lassen sich die Anforderungen an eine sichere Multifaktor-Authentifizierung wirtschaftlich umsetzen?

Die am 16. Januar 2023 in Kraft getretene EU-Richtlinie NIS2 (EU 2022/2555) ist ein zentraler Pfeiler der europäischen Cybersicherheitsstrategie. Bis zum 17. Oktober 2024 muss die Direktive in nationales Recht umgesetzt werden. Neben strengeren Meldepflichten bei Sicherheitsvorfällen verpflichtet NIS2 die betroffenen Unternehmen zu einem verbesserten Risikomanagement und verschärften Sicherheitsanforderungen. Von besonderer Bedeutung für die Praxis ist dabei die Einführung einer **Zugriffskontrolle** zu IT-Systemen und Netzwerken. Viele EU-Länder, darunter auch Deutschland, schreiben hierfür eine **Multi-Faktor-Authentifizierung** (MFA) vor[1]. Im Folgenden erfahren Sie, wie Sie dieses Verfahren wirtschaftlich umsetzen und empfindliche Strafen vermeiden. Übrigens: Ganz unabhängig vom Inkrafttreten der nationalen Gesetzgebung gilt die NIS2-Richtlinie unmittelbar ab dem 18. Oktober 2024, selbst wenn nationales Recht noch nicht umgesetzt ist.

Inhalt

1. Ist mein Unternehmen betroffen?

Die erste Fassung der NIS-Richtlinie wurde 2016 eingeführt, um das Sicherheitsniveau von Netzwerken und Informationssystemen in der Europäischen Union zu erhöhen. Mit NIS2 sollen kritische Infrastrukturen und wichtige digitale Dienste noch umfassender vor Cyberbedrohungen geschützt werden. Dazu erweitert NIS2 den bisherigen Kreis der sogenannten „KRITIS-Unternehmen" deutlich. Allein in Deutschland sind rund 29.000 Unternehmen zusätzlich betroffen. Zum erweiterten KRITIS-Kreis zählen hier neben Bundeseinrichtungen und Einrichtungen der Kritischen Infrastruktur auch solche, die als „wesentlich" oder „wichtig" für das staatliche Gemeinwesen eingestuft sind. In die Kategorie „wesentlich" für das staatliche Gemeinwesen fallen Bereiche wie Energie, Transport, Finanzen oder Gesundheit. Als „wichtig" gelten Postdienste, Abfallwirtschaft, Lebensmittel, Chemie, digitale Dienste oder Industrie- und Forschungseinrichtungen.

Neu ist auch: Während „wesentliche" und „wichtige" Einrichtungen erst ab einer bestimmten Mitarbeiter- oder Umsatzgröße betroffen sind, gilt NIS2 ausnahmslos für Anbieter von DNS-Diensten und Top-Level-Domain-Namensregistern sowie für Betreiber öffentlicher elektronischer Kommunikationsnetze oder -dienste. Darüber hinaus sollten sich alle Unternehmen mit NIS2 befassen, die Teil der Lieferkette einer direkt betroffenen Einrichtung sind. Denn diese können im Schadensfall eine Haftungsübernahme verlangen.

[1] §30 Absatz 4, Satz 9 und 10 NIS2UmsuCG (Referentenentwurf, Bearbeitungsstand 03.07.2023, veröffentlicht von der ag.kritis)

2. Welche Strafen drohen?

Ähnlich wie schon bei der EU-Datenschutzrichtlinie drohen Unternehmen sowie Vereinen und gemeinnützigen Gesellschaften harte Sanktionen, wenn sie gegen die NIS2-Vorschriften verstoßen. Die Maximalstrafe beträgt für „wesentliche" Einrichtungen **bis zu 10 Mio. Euro** oder **2 % des weltweiten Jahresumsatzes**, „wichtige" Einrichtungen haften mit bis zu 7 Mio. Euro bzw. 1,4 %. Unter Umständen muss die Geschäftsführung bzw. der Vorstand auch mit einer **persönlichen Haftung** rechnen[2]. Insofern sind Vorkehrungen im Bereich Cyber-Security vergleichbar mit einer Haftpflichtversicherung: Erst im Schadensfall wird klar, wie wichtig die Investition gewesen wäre.

Warum Sie bei der IT-Sicherheit
kein Risiko eingehen sollten?
Lesen Sie unser **Zero Trust Whitepaper**

3. Pflicht zur Zugriffskontrolle

Nicht nur für die NI2-Umsetzung gilt: Cybersicherheit ist eine Managementaufgabe und darf nicht delegiert werden. Wie also müssen sich die Unternehmen auf die neuen Cyber-Security-Anforderungen vorbereiten, um Sicherheits- und Haftungsrisiken zu vermeiden? Eine der wesentlichen Anforderungen von NIS2 besteht darin, geeignete Konzepte für die Zugriffskontrolle zu entwickeln. Der Grund liegt auf der Hand: Sichere IT-Strukturen fangen mit der Frage an, wer Zugang zu den einzelnen Systemen und Netzwerken hat. Vor unberechtigtem Zugriff zu schützen sind insbesondere:

- lokale Zugriffe auf PCs
- Fernzugriffe über VPN
- App-Zugriffe auf Cloud-basierte und lokale Anwendungen

Viele nationale NIS2-Umsetzungen, wie zum Beispiel der Referentenentwurf des deutschen NIS2-Umsetzungsgesetz NIS2UmsuCG, fordern zur Zugriffskontrolle explizit die Einführung einer Multi-Faktor-Authentifizierung[3]. Je nach EU-Mitgliedsland sind im Einzelnen die nationalen Vorgaben für den eingeschränkten IT-Zugriff zu prüfen.

Zugriffskontrolle

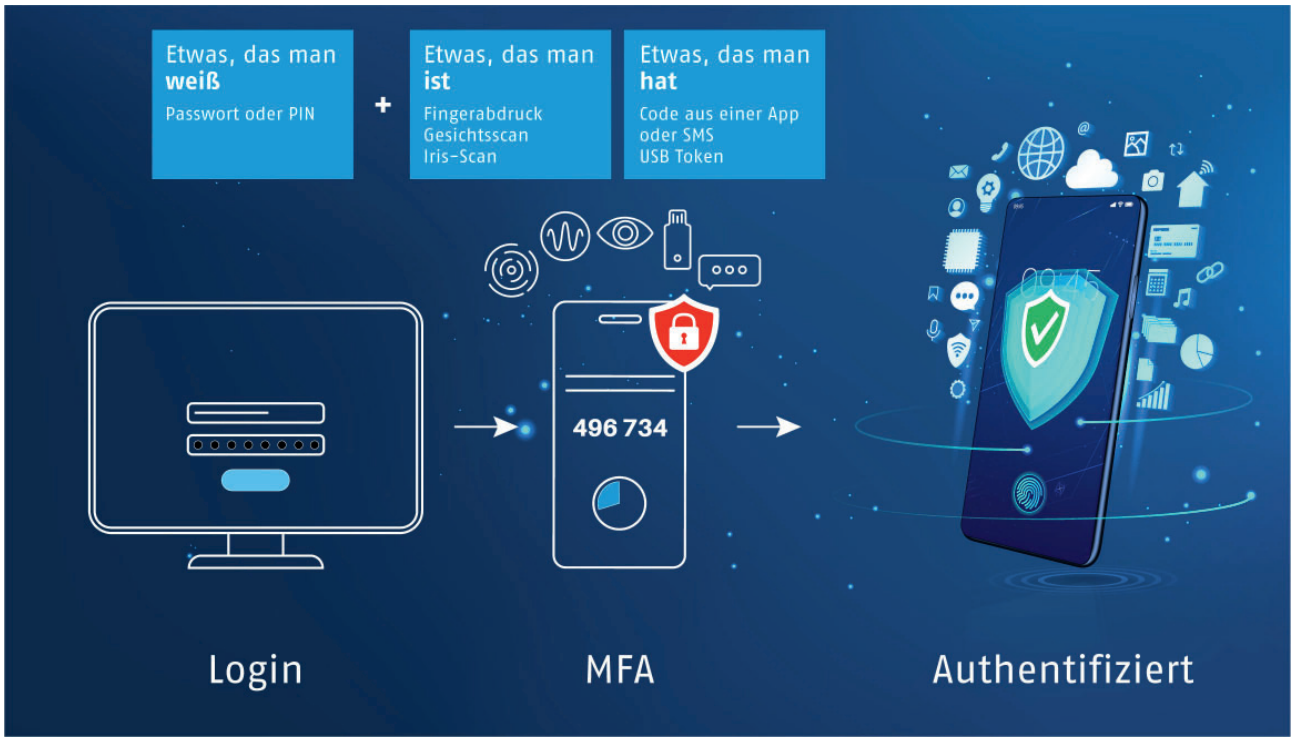
Im Kontext der NIS2-Richtlinie ist die Zugangskontrolle ein wesentliches Element zur Gewährleistung der Integrität, Verfügbarkeit und Vertraulichkeit von Netz- und Informationssystemen. Diese sind unerlässlich, um kritische gesellschaftliche und wirtschaftliche Funktionen aufrecht zu erhalten. Eine wirksame Zugriffskontrolle verringert das Risiko von Cyber-Angriffen, Datenlecks und anderen Sicherheitsvorfällen. Entsprechende Maßnahmen und Technologien stellen sicher, dass nur berechtigte Personen Zugriff auf bestimmte Informationen, Ressourcen oder Bereiche innerhalb eines Netzwerks oder Informationssystems haben. Eine Multi-Faktor-Authentifizierung stellt dies durch eine Kombination aus Wissenskomponenten wie Passwörter, biometrische Merkmale oder Besitzkomponenten wie Smartphones, Smartcards oder USB-Tokens sicher.

[2] https://www.security-insider.de/persoenliche-haftungsrisiken-aus-der-eu-richtlinie-nis2-a-42f0b436de2c7f83633656b144b43f2f/ (abgerufen am 01.03.2024)

[3] Referentenentwurf NIS2UmsuCG §30 (4) 9. & 10.

4. Multi-Faktor-Authentifizierung

Länder wie Deutschland schreiben in ihrer NIS2-Umsetzung für die Zugriffskontrolle eine Multifaktor-Authentifizierung (MFA) vor. Dieses Verfahren ist besonders effektiv, weil es sich nicht allein auf Wissensfaktoren wie PINs oder Passwörter stützt, sondern weitere Faktoren wie Besitz oder biometrische Merkmale fordert. Besitzkomponenten können hardwarebasiert sein, zum Beispiel ein USB-Token, eine Smartcard oder ein Smartphone. Softwarebasierte MFA-Lösungen nutzen hingegen Smartphone-Apps, SMS oder E-Mails zum Versenden generierter Zugriffscodes.



Zusätzliche Schutzebene: Die Multi-Faktor-Authentifizierung (MFA) verlangt mindestens zwei Identitätsnachweise für den IT-Zugriff.

5. Smartphone oder USB-Token?

Grundsätzlich gilt: Auch eine schlechte MFA ist besser als keine. Hinsichtlich Sicherheit, Praktikabilität und Wirtschaftlichkeit gibt es aber große Unterschiede. So sind etwa Token-basierte MFA-Lösungen aufgrund ihrer zusätzlichen Hardwarekomponente und eines je nach Protokoll integrierten Anti-Phishing-Schutzes als sicherer zu bewerten als Smartphone-basierte Lösungen. Eine SMS mit einem übermittelten Zugangscode können Hacker abfangen oder das Betriebssystem des Smartphones kompromittieren. Dagegen bieten MFA-Lösungen mit USB-Token und modernen Authentifizierungsprotokollen wie FIDO2 oder PIV eine deutlich kleinere Angriffsfläche.

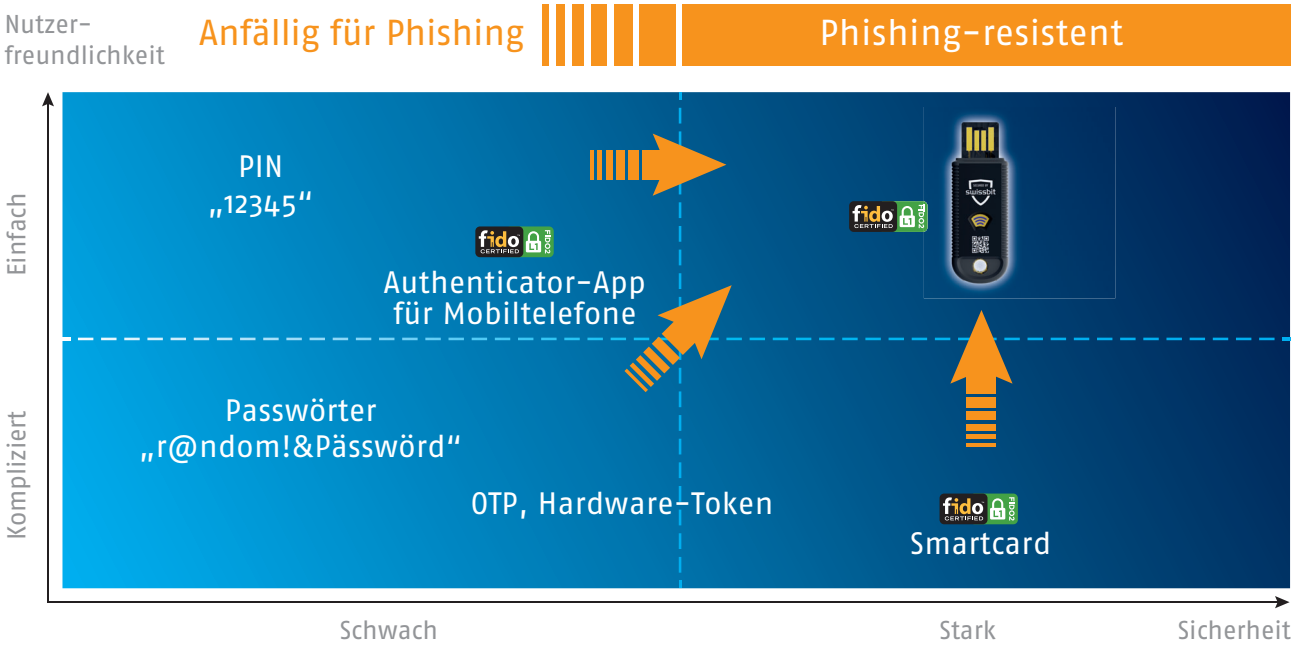
Passwortloser IT-Zugang

Der weltweit verbreitete Standard **FIDO2** ermöglicht sichere passwortlose Anmeldeverfahren für Computersysteme, Unternehmensnetzwerke, Websites und Apps. FIDO2 ist eine Initiative der FIDO Allianz mit dem World Wide Web Consortium (W3C), die von Unternehmen wie Apple, Microsoft und Google unterstützt wird. Mit FIDO2-kompatiblen Tokens können Unternehmen sehr einfach Phishing-resistente MFA-Lösungen implementieren.

Mehr: fidoalliance.org/fido2/

Ein weiterer Vorteil des USB-Tokens gegenüber dem Smartphone sind die deutlich niedrigeren Investitionskosten. Für den Preis eines durchschnittlichen Smartphones kann der Einkauf etwa 20 bis 30 Personen mit Token ausrüsten. Ein erheblicher Kostenfaktor, wenn die gesamte Belegschaft NIS2-konform ausgestattet werden soll. Hinzu kommen die hohen Lebenszykluskosten der Smartphones einschließlich Vorbereitung, Wartung und Gerätetausch.

Zudem lassen sich USB-Token leichter mit den Unternehmensrichtlinien in Einklang bringen als Smartphone-basierte Lösungen. Manche Mitarbeiterinnen und Mitarbeiter möchten keine dienstlichen Smartphones, geschweige denn ihre privaten Smartphones für die Authentifizierung im beruflichen Kontext nutzen. Ein USB-Token hingegen lässt sich leicht verpflichtend einführen und bietet damit eine sehr einfache und konsistente Basis für die Einführung von MFA.



Vor- und Nachteile unterschiedlicher MFA-Verfahren

6. Risiken vermeiden, Kosten sparen

Die Umsetzung von NIS2 in nationales Recht nimmt die Geschäftsführung von KRITIS-Unternehmen persönlich in die Pflicht, ihre IT-Systeme vor unberechtigten Zugriffen zu schützen. Die Erfahrungen der letzten Jahre mit der Datenschutz-Grundverordnung zeigen, dass bei der strafrechtlichen Verfolgung nicht mit Nachsicht zu rechnen ist. Betroffene Unternehmen sollten jetzt handeln, um Fristen einzuhalten, empfindliche Strafen zu vermeiden und die Sicherheit ihrer IT-Umgebung wirksam vor unberechtigten Zugriffen zu schützen.

Wer beim wichtigen NIS-Thema Multifaktor-Authentifizierung rechtlich, technisch und wirtschaftlich auf der sicheren Seite sein will, ist mit USB-Token-basierten Lösungen wie dem **iShield Key von Swissbit** gut beraten. Diese sind nicht nur deutlich kostengünstiger und einfacher zu bedienen als Smartphone-basierte Lösungen, sondern bieten einschließlich Anti-Phishing auch die bestmögliche Sicherheit.

Sie möchten sich unverbindlich über NIS2, MFA und USB-Tokens informieren? Kontaktieren Sie uns unter:
swissbit.com/kontakt

swissbit®

Effizient und sicher: iShield Key von Swissbit

Die Hardware-basierte MFA-Lösung iShield Key Pro von Swissbit bietet die bestmögliche Sicherheit für den NIS2-konformen Zugriff auf Websites, Anwendungen, Dienste und Unternehmensnetzwerke. Die starke hardwarebasierte Authentifizierungsmöglichkeit Made in Germany bietet einen kostengünstigen und sicheren Schutz vor Online-Angriffen wie Phishing, Social Engineering oder Kontoübernahmen. Der iShield Key Pro kann selbst Smartphones mit Authenticator App ersetzen, da er fleixbelflexibel mit folgenden Standards eingesetzt werden kann:

- FIDO & FIDO2: Phishing-resistente Multi-Faktor-Authentifizierung, Basis für Zero-Trust-Architekturen
- PIV: elektronische Signatur für PDFs und E-Mails
- HTOP & TOTP: für nicht-FIDO-kompatible Legacy- und Bestandssysteme

Mehr erfahren:

swissbit.com/ishield-key

Autoren

Alexander Summerer
Head of Authentication

Stefan Gockel
Key Account Manager Embedded IoT Solutions

Haben Sie Fragen? Kontaktieren Sie uns:

Swissbit Europe (HQ)
Tel. +41 71 913 03 00
sales@swissbit.com

Swissbit North America
Tel. +1 978-490-3252
salesna@swissbit.com

Swissbit Japan
Tel. +81 3 6258 0521
sales-japan@swissbit.com

Swissbit Asia
Tel. +886 912 059 197
salesasia@swissbit.com

Über Swissbit

Die Swissbit AG ist der führende europäische Anbieter von Speicherprodukten, Sicherheits- und Embedded-IoT-Lösungen für anspruchsvolle Anwendungen. Swissbit entwickelt und produziert industrietaugliche Speicher- und Security-Produkte „Made in Germany" mit höchster Zuverlässigkeit, Langzeitverfügbarkeit und kundenspezifischer Optimierung.

www.swissbit.com

Änderungen vorbehalten.