swissbit®

White Paper

Multifaktor-Authentifizierung: NIS2-Anforderungen erfüllen, Haftungsrisiken vermeiden.

Sicheres Access Management.

© Swissbit AG 2026. Alle Rechte vorbehalten.



swissbit®

Schützen Sie Ihren digitalen & physischen Zugang

iShield Key 2



fido CERTIFIED FIDO2 L2

140-3 FIPS

MIFARE

HID SEOS

LEGIC

Made in Germany

swissbit®

Die NIS2-Richtlinie der Europäischen Union stellt seit Januar 2023 hohe Anforderungen an die Cybersicherheit kritischer Infrastrukturen besonders wichtiger sowie wichtiger Einrichtungen. Sie adressiert zahlreiche Unternehmen, Behörden und Organisationen. Zum Schutz der Integrität ihrer Systeme sind adäquate technische wie organisatorische Maßnahmen vonnöten. Andernfalls drohen je nach Haftungsrisiko empfindliche Geldbußen. Eine sichere Multi-Faktor-Authentifizierung ist strategischer Konsens. Für Unternehmen rückt die Wirtschaftlichkeit des konkreten Setups zunehmend in den Fokus.

Die EU-Richtlinie NIS2 (EU 2022/2555) ist ein zentraler Pfeiler der europäischen Cybersicherheitsstrategie. In Deutschland trat das NIS2-Umsetzungsgesetz im Dezember 2025 in Kraft. Es verschärft die Melde- und Registrierungspflichten für KRITIS und andere besonders kritische Einrichtungen. Auch Unternehmen mit wesentlicher Bedeutung für Wirtschaft und Gesellschaft, etwa Banken, IT-Dienstleister sowie die Wasser- und Abfallwirtschaft, müssen umfassendes Risikomanagement und angemessene technische und organisatorische Sicherheitsmaßnahmen umsetzen. Eine entscheidende Rolle spielen dabei Zugriffskontrollen und sichere Authentifizierungsverfahren. Das BSI-Gesetz nennt ausdrücklich Lösungen wie Multi-Faktor-Authentifizierung (MFA) und kontinuierliche Authentifizierung. Im Folgenden zeigen wir, welche Unternehmen betroffen sind, welche Anforderungen gelten und wie sich MFA sicher und wirtschaftlich umsetzen lässt.



Inhalt

1. NIS2 endet nicht an der Unternehmensgrenze
2. Empfindliche Strafen. Klare Verantwortung
3. Sicherheit beginnt bei Access Control
4. MFA: Mehr Hürden. Weniger Schwachstellen.
5. Der zweite Faktor macht den Unterschied.
6. Regulatorik trifft Unternehmensrealität
7. Der Schlüssel zu mehr Sicherheit.

1. NIS2 endet nicht an der Unternehmensgrenze

Die erste Fassung der NIS-Richtlinie wurde 2016 eingeführt, um das Sicherheitsniveau von Netzwerken und Informationssystemen in der Europäischen Union zu erhöhen. Mit NIS2 wurde der Anwendungsbereich deutlich erweitert, um kritische Infrastrukturen und wichtige digitale sowie wirtschaftliche Dienste umfassender vor Cyberbedrohungen zu schützen. In Deutschland unterscheidet das BSI-Gesetz unter anderem zwischen besonders wichtigen und wichtigen Einrichtungen. Darunter fallen zahlreiche Unternehmen aus Bereichen wie Energie, Verkehr, Finanzwesen, Gesundheitswesen, digitale Infrastruktur und öffentliche Verwaltung sowie unter anderem Unternehmen aus Post- und Kurierdiensten, Abfallwirtschaft, Lebensmittelwirtschaft, Chemie, Produktion und Forschung. Neben der Branche bestimmen insbesondere Unternehmensgröße, Mitarbeiterzahl sowie Umsatz bzw. Bilanzsumme, für wen die Regelungen gelten. Für einzelne Einrichtungen gelten unabhängig davon besondere Vorgaben. Auch nicht unmittelbar betroffene Unternehmen sind über ihre Lieferketten und Dienstleisterbeziehungen mittelbar gefordert. NIS2 macht deren Sicherheit zum Bestandteil des holistischen Risikomanagements und erhöht damit auch die Anforderungen an Zulieferer und IT-Dienstleister.

2. Empfindliche Strafen. Klare Verantwortung.

Nachhaltige Investitionen in die Cybersicherheit sind nicht nur eine technische Herausforderung, sondern integraler Bestandteil eines angemessenen unternehmerischen Risikomanagements. Verstöße gegen die gesetzlichen Vorgaben sind mit erheblichen finanziellen Folgen verknüpft. Für besonders wichtige Einrichtungen drohen Bußgelder von bis zu 10 Millionen Euro oder 2 % des weltweiten Jahresumsatzes, für wichtige Einrichtungen mit einem weltweiten Jahresumsatz über 500 Millionen Euro sind es bis zu 7 Millionen Euro oder 1,4 %. Maßgeblich ist jeweils der höhere Betrag. Auch die Geschäftsleitung steht in der Verantwortung. Sie muss die vorgeschriebenen Risikomanagementmaßnahmen umsetzen und ihre Einhaltung überwachen. Werden diese Pflichten schuldhaft verletzt, drohen persönliche Haftungsrisiken nach den jeweils geltenden gesellschaftsrechtlichen Regelungen.

3. Sicherheit beginnt bei Access Control.

Cybersicherheit ist mit NIS2 zur Managementaufgabe geworden. Entscheidend ist, Zugriffe konsequent abzusichern und sicherzustellen, dass nur autorisierte Personen auf sensible Daten, Anwendungen und Infrastrukturen zugreifen können.

Das erfordert klare Zugriffskontrollen für:
- lokale Zugriffe auf PCs und Workstations
- Fernzugriffe über VPN
- Cloud- und lokale Anwendungen
- administrative und besonders sensible Systeme

Das BSI-Gesetz nennt neben Zugriffskontrollkonzepten ausdrücklich auch Multi-Faktor-Authentifizierung und kontinuierliche Authentifizierung als mögliche Risikomanagementmaßnahmen. Für eine besonders hohe Phishing-Resistenz kommen gerätegebundene Passkeys auf FIDO2-Security-Keys zum Einsatz. Sie verknüpfen die Identität mit einem physischen Sicherheitsgerät und schützen so insbesondere vor Phishing- und Adversary-in-the-Middle-Angriffen. Welche Lösung im Einzelfall geeignet ist, hängt vom individuellen Risikoprofil und den eingesetzten Systemen ab.

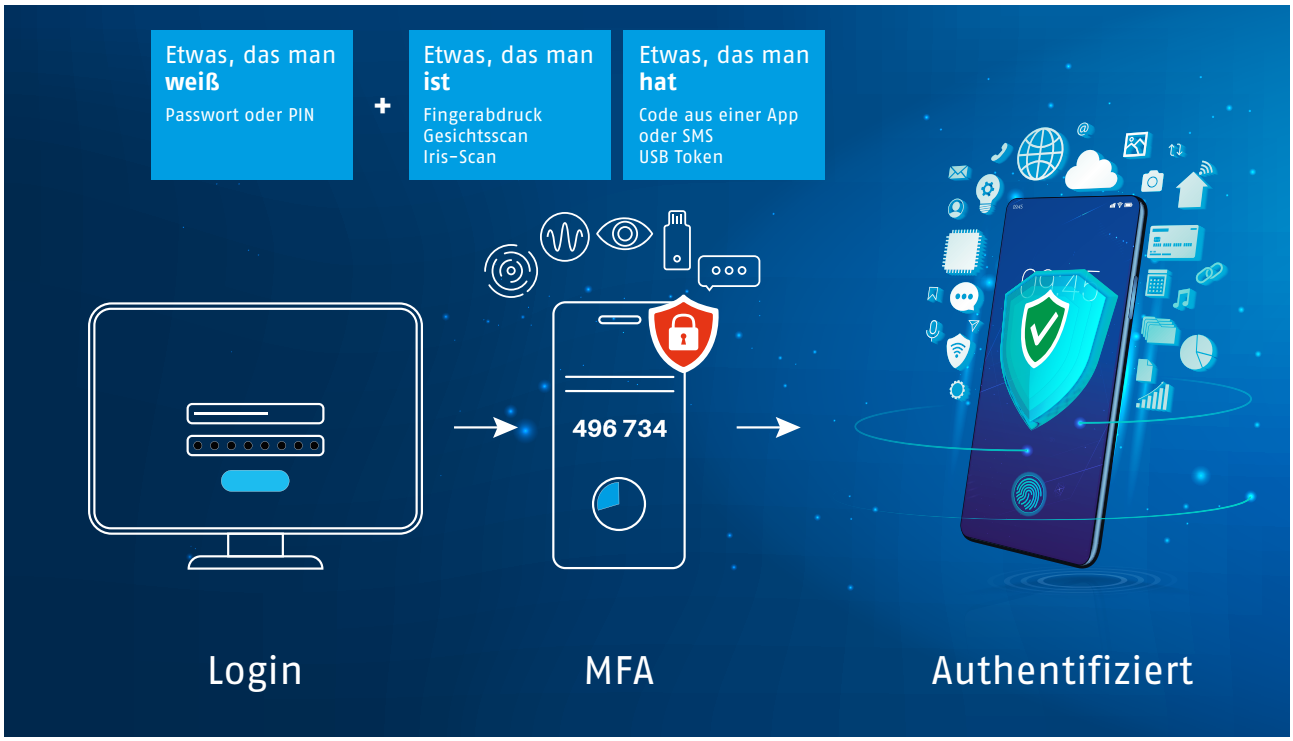


Zugriffskontrolle

Im Kontext von NIS2 ist Zugriffskontrolle ein zentraler Baustein, um Vertraulichkeit, Integrität und Verfügbarkeit von Netz- und Informationssystemen zu gewährleisten. Sie stellt sicher, dass nur autorisierte Personen auf definierte Informationen, Ressourcen und Systeme zugreifen können, und reduziert damit das Risiko von Cyberangriffen, Datenlecks und weiteren Sicherheitsvorfällen. Multi-Faktor-Authentifizierung erhöht das Schutzniveau zusätzlich, indem mehrere voneinander unabhängige Authentifizierungsfaktoren kombiniert werden: etwa Wissen (Passwort), Besitz (Smartphone, Smartcard oder Security Token) oder ein biometrisches Merkmal.

4. MFA: Mehr Hürden. Weniger Schwachstellen.

In Deutschland ist Multi-Faktor-Authentifizierung (MFA) in den nach § 30 BSIG geforderten Risikomanagement-maßnahmen verankert. Ihr entscheidender Vorteil: Kompromittiert ein Angreifer einen Faktor, reicht dieser allein nicht für den Zugriff. Dabei ist MFA nicht gleich MFA: Je nach Verfahren bietet der zweite Faktor unterschiedlich viel Schutz vor gezielten Phishing- und Man-in-the-Middle-Angriffen. Während SMS- oder E-Mail-Codes abgefangen werden können, gelten FIDO2-basierte Verfahren als phishing-resistent. Entscheidend ist daher nicht allein, ob MFA eingesetzt wird, sondern wie sicher der gewählte Faktor tatsächlich ist.



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

5. Der zweite Faktor macht den Unterschied.

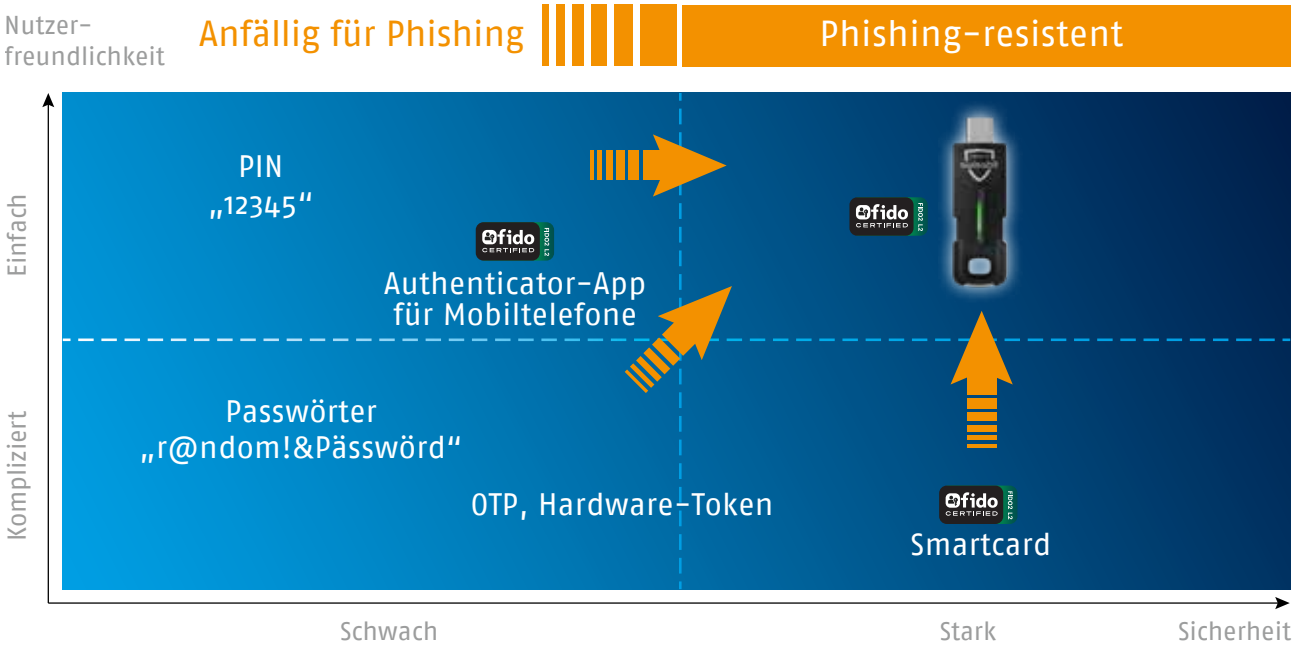
MFA erhöht das Sicherheitsniveau gegenüber einer reinen Passwortauthentifizierung deutlich. Doch wie bei einer Kette gilt: Die Sicherheit des Gesamtsystems hängt von der Qualität seiner einzelnen Faktoren ab. Wichtig ist, wie widerstandsfähig der gewählte zweite Faktor gegenüber aktuellen Angriffsmethoden ist. Einmalcodes können abgefangen oder über manipulierte Anmeldeseiten abgegriffen werden. Selbst softwarebasierte Verfahren bieten je nach Ausgestaltung unterschiedlich viel Schutz vor Phishing und anderen Angriffen auf Anmeldeprozesse.

Passwortloser IT-Zugang

FIDO2 ist ein international etablierter Standard für sichere, phishing-resistente und passwortlose Authentifizierung. Die FIDO Alliance entwickelt die zugrunde liegenden Standards, das W3C standardisiert mit WebAuthn deren webbasierte Umsetzung. FIDO2 wird von zahlreichen Technologieunternehmen unterstützt und ermöglicht sichere Anmeldungen an Systemen, Netzwerken, Websites und Anwendungen. FIDO2-kompatible USB-Token nutzen diese Stärken in einem dedizierten Authentifizierungsgerät.

Mehr: fidoalliance.org/fido2/

FIDO2-basierte Authentifizierung setzt hier einen anderen Sicherheitsmechanismus ein. Der private kryptografische Schlüssel bleibt auf dem Authentifizierungsgerät und wird nicht an einen Dienst übertragen. Das erhöht den Schutz vor Phishing deutlich. USB-Token bieten dabei einen dedizierten Besitzfaktor, der unabhängig vom Smartphone eingesetzt werden kann. Denn auch das Smartphone kann zur Angriffsfläche werden. Sein Einsatz für Authentifizierungszwecke bringt zusätzliche Anforderungen an Beschaffung, Einrichtung, Verwaltung, Wartung und Gerätetausch mit sich. Ein USB-Token reduziert diese Abhängigkeit und lässt sich unabhängig von privaten Endgeräten konsistent im Unternehmen einsetzen. Damit verschiebt sich die Frage: Nicht nur, ob MFA eingesetzt wird, sondern wie widerstandsfähig der zweite Faktor ist – und wie sich dieses Sicherheitsniveau skalierbar umsetzen lässt.



Vor- und Nachteile unterschiedlicher MFA-Verfahren

6. Regulatorik trifft Unternehmensrealität

Mit der Umsetzung von NIS2 in deutsches Recht sind auch die Geschäftsleitungen besonders wichtiger und wichtiger Einrichtungen stärker in die Verantwortung gerückt. Sie müssen die erforderlichen Risikomanagementmaßnahmen vorantreiben und deren Umsetzung überwachen. Damit wird Cybersicherheit zur strategischen Unternehmensaufgabe: Gefordert sind Lösungen, die regulatorischen Anforderungen gerecht werden und sich zugleich dauerhaft, wirtschaftlich und verlässlich in den Unternehmensalltag integrieren lassen.

Der iShield Key 2 von Swissbit verbindet beides. Als FIDO2-basierte Hardwarelösung schafft er eine belastbare Grundlage für eine moderne, regulatorisch anschlussfähige MFA-Strategie – und ermöglicht deren konsistente Umsetzung über Nutzer, Systeme und Standorte hinweg. So wird aus einer gesetzlichen Verpflichtung eine langfristig tragfähige und wirtschaftliche Sicherheitsarchitektur.

7. Der Schlüssel zu mehr Sicherheit.

Die hardwarebasierte MFA-Lösung iShield Key 2 von Swissbit schafft eine belastbare Grundlage für sichere Zugriffe auf Websites, Anwendungen, Dienste und Unternehmensnetzwerke. Die Authentifizierung über dedizierte Hardware verbindet FIDO2-Technologie mit passwortlosen Passkeys und schützt vor Phishing, Social Engineering und Accountübernahmen. So entsteht eine moderne Zugriffsarchitektur, die hohe Sicherheitsanforderungen mit einer konsistenten Umsetzung im Unternehmen verbindet.

Als führender Value Added Distributor unterstützt ADN Sie umfassend von der Beratung über das Proof of Concept bis hin zur reibungslosen Bereitstellung und Integration in Ihre Infrastruktur.



Glossar

FIDO2 & Passkeys: Phishing-resistente, passwortlose Multi-Faktor-Authentifizierung mit bis zu 300 gespeicherten Passkeys

Zero Trust: Starke Identitätsprüfung und Zugriffskontrolle für moderne IT-Umgebungen

Flexible Integration: USB-A, USB-C und NFC für bestehende Unternehmensumgebungen

Skalierbarer Betrieb: Einheitliche Hardware für die unternehmensweite Ausrollung

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.

© Swissbit AG 2026. Alle Rechte vorbehalten.