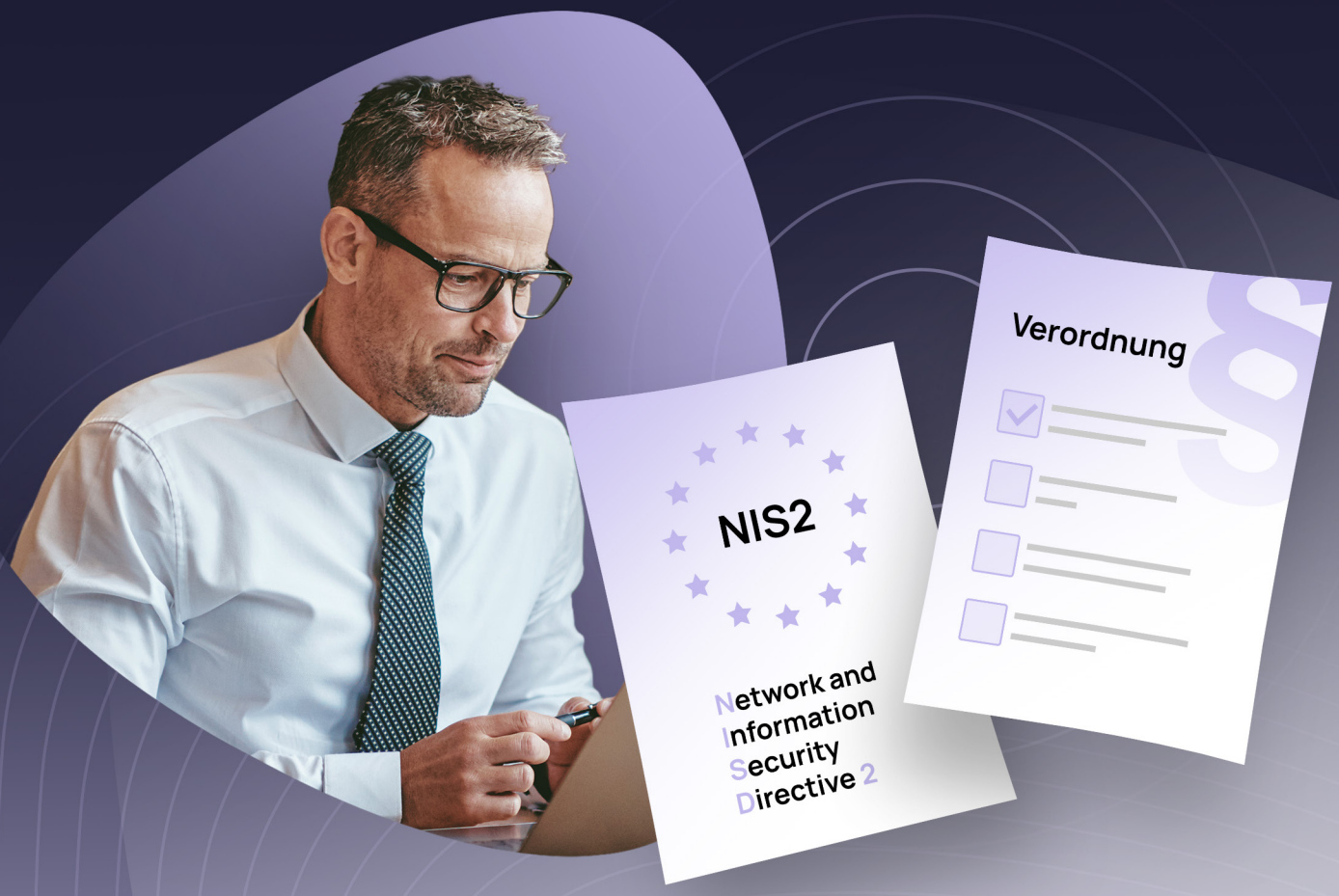
sosafe

NIS2 auf den Punkt gebracht: Was die Richtlinie für Ihre Organisation bedeutet

> Wie die NIS2-Richtlinie den Anstieg immer ausgefeilterer Cyberangriffe bekämpfen soll



NIS2

Die NIS2-Richtlinie ist ein zentrales Regelwerk, mit dem die Cybersicherheit und der Schutz kritischer Infrastrukturen innerhalb der Europäischen Union (EU) entscheidend gestärkt werden. Ihr Ziel ist es, kritische Sektoren durch die Festlegung strengerer Cybersicherheitsstandards zu schützen, aber sie konzentriert sich auch auf Rapid Incident Reporting und eine bessere Zusammenarbeit zwischen den EU-Mitgliedern im Bereich der Cybersicherheit.

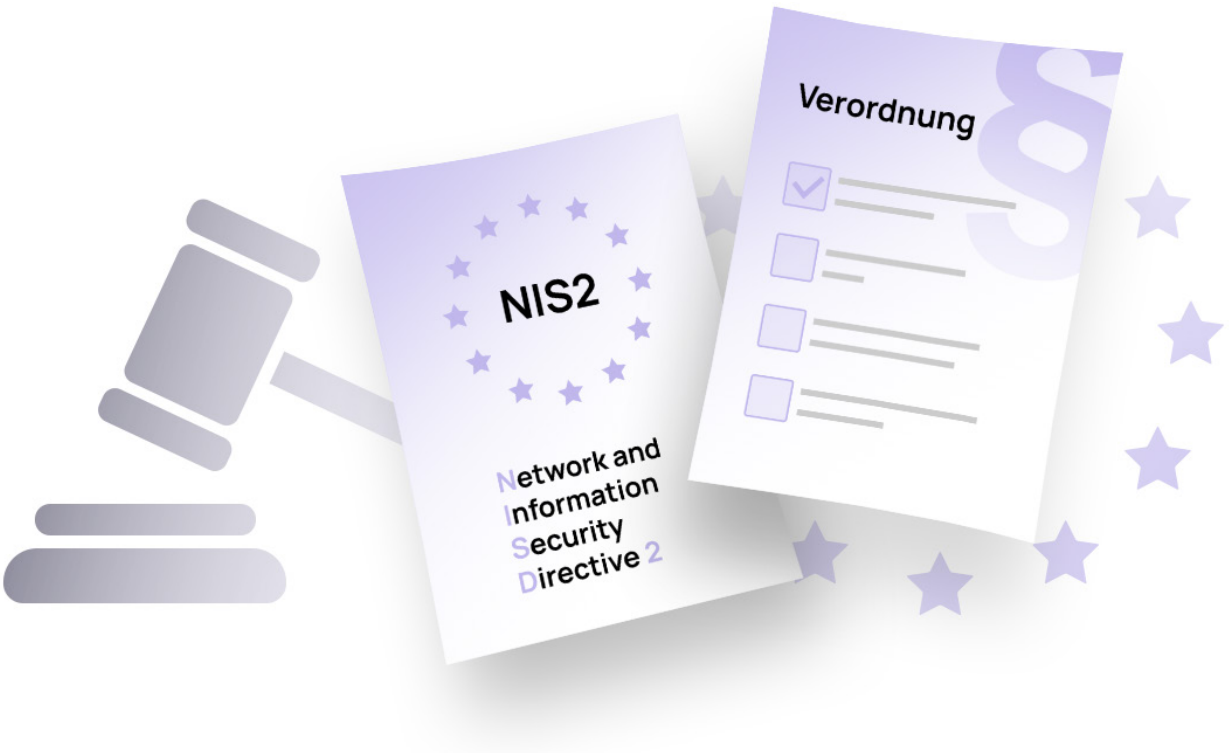
Inhalt

Was ist NIS2?

Die NIS2-Richtlinie, die Nachfolgerin der ursprünglichen Richtlinie für die Netz- und Informationssicherheit, ist ein zentrales Regelwerk, mit dem die **Cybersicherheit und der Schutz kritischer Infrastrukturen innerhalb der Europäischen Union (EU) entscheidend gestärkt werden**. Die NIS2-Richtlinie beseitigt die Defizite ihrer Vorgängerin und erweitert ihren Geltungsbereich. Sie definiert strengere Sicherheitsvorgaben, stärkt das Meldewesen und optimiert das Krisenmanagement.

Um die Notwendigkeit und Relevanz der NIS2-Richtlinie zu verstehen, muss man sich ein umfassendes Bild über unser immer stärker vernetztes digitales Ökosystem verschaffen. Die digitale Infrastruktur in Europa ist weitläufig und komplex und berührt nahezu jeden Aspekt des modernen Lebens und Handels. Diese Vernetzung verspricht außergewöhnliche Wachstumsmöglichkeiten und Effizienzgewinne, öffnet aber auch Türen für eine Vielzahl potenzieller Cyberbedrohungen und Schwachstellen.

Durch die Stärkung der digitalen Verteidigungslinie, die von der ursprünglichen NIS-Richtlinie aus dem Jahr 2016 geschaffen wurde, und die Erweiterung des Geltungsbereichs fungiert die NIS2-Richtlinie als starke Festung in der aktuellen Cyber-Bedrohungslage. Die im Jahr 2022 eingeführte **NIS2-Richtlinie reagiert auf den Anstieg von immer ausgefeilteren und schwerwiegenderen Cyber-angriffen** und definiert eine solide, umfassende und adaptierbare Verteidigungsstrategie.



Warum NIS2? Ein Blick auf die aktuelle Bedrohungslage in Europa

Angetrieben durch die Innovationskraft der Cyberkriminellen hat sich die Bedrohungslage in jüngster Zeit stark verschärft. Technologische Neuerungen, insbesondere KI-Tools, tragen entscheidend zu immer komplexeren und nahtlos umgesetzten Bedrohungen bei. Gepaart mit der wachsenden Professionalisierung der Cyberkriminalität können Angriffe einfacher denn je ausgeführt werden. Heute stehen Angreifenden sogar illegale Plattformen bereit, die ähnlich wie konventionelle SaaS-Angebote funktionieren.

Einen weiteren Aspekt der komplexen Bedrohungslage bilden globale Spannungen und nationale Konflikte, die verstärkt im digitalen Raum ausgetragen werden. Staatlich finanziertes Hacking, Cyber-Spionage und Cyber-Kriegsführung etablieren sich mittlerweile als potente Tools, was die Bedrohungslage weiter anspannt. Und auch der starke Anstieg von Remote Work spielt Cyberkriminellen durch ungeschützte private Endgeräte und unzuverlässige Verbindungen unfreiwillig in die Karten.

Unser Human Risk Review 2023 hat diese Trends bestätigt: 3 von 4 Sicherheitsverantwortlichen sagen, dass sich das Cyberrisiko ihrer Organisation aufgrund der geopolitischen Verflechtungen, die Verbreitung von KI und die Umstellung auf Remote Work erhöht hat. Hinzu kommt, dass jede zweite Organisation bereits Opfer eines Cyberangriffs wurde und ein Drittel der Sicherheitsexperten in absehbarer Zukunft mit weiteren Angriffen rechnen.

Diese Zunahme von Cyberbedrohungen gefährdet besonders Schlüsselindustrien und wichtige Branchen. Diese sind vor allem daher lohnenswerte Ziele für Cyberkriminelle, da hier jede Serviceunterbrechung sofort behoben werden muss. Diese Dringlichkeit macht sie anfällig für Erpressung durch böswillige Akteure, die sich finanziell bereichern wollen, was die Daten von Statista aus dem Jahr 2022 belegen. Sie zeigen deutlich, dass Energie, Bildung, Gesundheitswesen, Behörden, Verkehr sowie Medien und Telekommunikation die Sektoren sind, die am häufigsten von Cyberangriffen betroffen sind.

Als Reaktion auf die Heftigkeit dieses Cyber-Sturms wurden Rechtsvorschriften wie die NIS2-Richtlinie und DORA eingeführt. Diese Gesetzesinitiativen fungieren als Leuchtturm, der europäischen Organisationen die Navigation durch diese turbulenten Gewässer erleichtert. Primäres Ziel ist dabei die Unterstützung eines koordinierten Vorgehens, um Organisationen zu ermöglichen, die immer neuen Cyberbedrohungen effektiver zu bekämpfen.

Was sind die Ziele der NIS2-Richtlinie?

NIS2 geht in Sachen digitaler Resilienz und Bedrohungsmanagement einen Schritt weiter. Über die Stärkung der Cybersicherheit hinaus dient NIS2 als Roadmap für störungsfreie Geschäftsabläufe, die Optimierung der Zusammenarbeit und die Förderung einer Sicherheitskultur, in der die Mitarbeitenden sichere Verhaltensweisen verinnerlichen. Mit NIS2 soll Folgendes erreicht werden:

Implementierung von Asset-Management-Verfahren, um kritische Informationssysteme und Ressourcen zu identifizieren und zu schützen

Beseitigung von Inkonsistenzen und Optimierung der Kommunikation und Zusammenarbeit zwischen den Mitgliedstaaten

Meldung von Vorfällen bei den zuständigen Stellen und Gewährleistung der effizienten Reaktion auf Zwischenfälle

Definition und Umsetzung von Cybersicherheitsstrategien sowie von Risikomanagement-Abläufen

Ausarbeitung von Protokollen für die Abwicklung von Vorfällen, von Vorgaben für das Meldewesen und von 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 im Hinblick auf optimale Cyber-Sicherheitsprotokolle

Zuverlässige Meldung von Vorfällen bei den zuständigen Stellen und Wahrung der schnellen Reaktionsfähigkeit

Von NIS zu NIS2: Was sind die wichtigsten Änderungen?

Die ursprüngliche NIS-Richtlinie wurde als Antwort auf die zunehmende Digitalisierung eingeführt, durch die neue, schwerwiegendere Cybersicherheitsrisiken für Organisationen und für die breite Öffentlichkeit entstanden. Diesen Risiken musste entgegengewirkt werden, um kritische Dienste, sensible Informationen und das Wohl der Menschen und der Wirtschaft zu schützen. Nach ihrer Einführung 2018 wurde die NIS-Richtlinie aber nicht einheitlich in den einzelnen Mitgliedstaaten umgesetzt. So entstand ein fragmentiertes System, in dem Organisationen den Anforderungen nicht oder nur zum Teil nachkamen. Einer der Hauptgründe dafür war, dass der Begriff „Betreiber wesentlicher Dienste" in den Staaten unterschiedlich definiert wurde. Daraus ergab sich die Notwendigkeit einer neuen, detaillierteren und verbesserten Rechtsvorschrift.

Im Anschluss an die nötige Überarbeitung der NIS-Richtlinie definierte die Europäische Kommission eine neue NIS2-Richtlinie, die die aktuellen Anforderungen des Markts berücksichtigt und die Unzulänglichkeiten der Vorgängerin beseitigte. Konkret heißt das, dass **NIS2 einen erweiterten Definitionsbereich** darüber hat, was als Betreiber wesentlicher Dienste gilt. Weitere Änderungen sind eine neue Verbindungsorganisation für Krisen, strengere Meldepflichten für Unternehmen, der Fokus auf die Sicherheit der Lieferkette, Anforderungen für die Cyberhygiene, Peer Reviews für die bessere Zusammenarbeit zwischen Mitgliedstaaten und eine Erweiterung der persönlichen Haftung von Leitungsorganen. Lesen Sie weiter, um mehr über diese Änderungen zu erfahren.

Zusätzliche Einrichtungen und Sektoren

Der Anwendungsbereich von NIS2 erstreckt sich auf zusätzliche Einrichtungen und umfasst nun auch Sektoren wie die Herstellung von chemischen Stoffen, die Produktion von medizinischen Geräten, die Verarbeitung von Lebensmitteln und die Bereitstellung von Diensten sozialer Netzwerke – alles Sektoren, die von der Vorgängerrichtlinie NIS nicht berücksichtigt wurden. In Artikel 3 der NIS2 werden die Klassifizierungen verfeinert. Hier werden abhängig von Größe und Sektor die Begriffe „Betreiber wesentlicher Dienste" und „Anbieter digitaler Dienste" durch „wesentliche Einrichtungen" und „wichtige Einrichtungen" ersetzt. Für diese Klassifizierungen gelten zwar ähnliche Pflichten, jedoch unterliegen wesentliche Einrichtungen einer stärkeren regulatorischen Kontrolle mit strengeren Durchsetzungsmaßnahmen. Die vollständige Liste der in NIS2 definierten Einrichtungen finden Sie weiter unten.

Europäisches Netzwerk der Verbindungsorganisationen für Cyberkrisen (EU-CyCLONe)

Gemäß Artikel 16 wird die Kommission eine EU-CyCLONe-Organisation einrichten, die aus Vertretern von EU-Ländern besteht und das Management von Cyber-Sicherheitsvorfällen unterstützt. Bei Bedarf werden auch Vertreter der Europäischen Kommission eingebunden. Hauptaufgabe der Organisation ist die Koordinierung des Umgangs der verschiedenen Länder mit Cyber-Sicherheitsvorfällen großen Ausmaßes durch Folgendes:

- Gewährleistung der optimalen Vorbereitung der Länder auf Cybersicherheitsvorfälle großen Ausmaßes und Krisen
- Entwicklung eines gemeinsamen Verständnisses darüber, was bei diesen Vorfällen und Krisen geschieht
- Bewertung der Folgen dieser Vorfälle und Vorschläge für mögliche Abhilfemaßnahmen
- Koordinierung des Managements dieser Vorfälle in den einzelnen Ländern und Unterstützung der Entscheidungsfindung auf politischer Ebene
- Erörterung und Unterstützung nationaler Pläne für die Reaktion auf Cyber-Sicherheitsvorfälle

Die NIS2-Richtlinie sieht außerdem die Einrichtung einer Kooperationsgruppe vor, die den reibungslosen Informationsaustausch und die effiziente Kooperation zwischen den Mitgliedstaaten ermöglicht. EU-CyCLONe erstattet der Kooperationsgruppe regelmäßig Bericht über Cyber-Sicherheitsvorfälle großen Ausmaßes sowie Trends, wobei der Schwerpunkt insbesondere auf deren Auswirkungen auf wesentliche Einrichtungen und Dienste liegt. Bis zum 17. Juli 2024 und danach alle 18 Monate übermittelt das EU-CyCLONe dem Europäischen Parlament und dem Rat einen Bericht, in dem es seine Arbeit bewertet.

Sicherheit von Lieferketten

Gemäß Artikel 22 der NIS2 sind Organisationen verpflichtet, die Sicherheit ihrer Lieferketten zu gewährleisten, einschließlich der Risiken, die durch die Lieferantenbeziehungen entstehen. Das ist ein essentieller Aspekt, da viele Cyberangriffe durch Schwachstellen in externen Lieferanten begünstigt werden. Organisationen müssen daher die Qualität und Resilienz der eingesetzten Produkte und Dienste untersuchen und sicherstellen, dass diese keine Schwachstelle für Betreiber wesentlicher Dienste darstellen. Organisationen sollten auch untersuchen, wie ihre externen Lieferanten das Thema Cybersicherheit angehen und ob ihre aktuellen Maßnahmen robust genug sind, um den Schutz der gesamten Lieferkette zu gewährleisten.

Einrichtungen, die wichtige Dienste für Mitgliedstaaten bereitstellen – wie z. B. DNS-Dienste, TLD-Namenregister, Domänennamen-Registrierung, Cloud-Computing, Rechenzentrumsdienste, Inhaltszustellnetze, verwaltete Dienste, verwaltete Sicherheitsdienste oder Online-Marktplätze, Suchmaschinen oder soziale Netzwerke – und ihren Sitz außerhalb der EU haben, müssen einen Vertreter in der Union benennen. Der Vertreter ist für die Compliance-Pflichten der Organisation im Rahmen der NIS2 und für die Meldung von Sicherheitsvorfällen verantwortlich.

Um ein einheitliches Cybersicherheitsniveau über alle Lieferanten hinweg zu gewährleisten und die Gefahr von Cybervorfällen zu reduzieren, müssen Betreiber wesentlicher Dienste die erforderlichen Maßnahmen in den Verträgen mit externen Lieferanten festhalten.

Strengere Meldepflichten

Um die schnelle Reaktion zu gewährleisten, sind betroffene Unternehmen gemäß Artikel 23 der NIS2 verpflichtet, das Computer Security Incident Response Team (CSIRT) oder ggf. eine zuständige nationale Behörde innerhalb von 24 Stunden nach dem Auftreten eines erheblichen Sicherheitsvorfalls zu benachrichtigen. Als erheblich gilt ein Sicherheitsvorfall, wenn er schwerwiegende Betriebsstörungen oder finanzielle Verluste für Einrichtungen zur Folge hat oder erhebliche materielle oder immaterielle Schäden für andere Personen verursacht. Bei Bedarf können Organisationen auch Unterstützung bei der Umsetzung von Abhilfemaßnahmen in Anspruch nehmen. Die zuständige Behörde wird auf die Meldung reagieren, Hilfe beim Umgang mit dem Vorfall anbieten und bei Bedarf andere betroffene Länder informieren.

Innerhalb von 72 Stunden nach Kenntnisnahme des Vorfalls stellt die betroffene Einrichtung Details über den Vorfall und eine erste Bewertung des erheblichen Sicherheitsvorfalls bereit. Spätestens einen Monat nach Übermittlung der Meldung des Sicherheitsvorfalls übermittelt die betroffene Organisation einen Abschlussbericht mit einer ausführlichen Beschreibung des Schweregrads des Vorfalls, der Auswirkungen und der Ursachen sowie den vom Unternehmen durchgeführten Abhilfemaßnahmen.

Cyberhygiene

Angesichts der immer komplexeren und anspruchsvolleren Cyberbedrohungen ist es für Organisationen von entscheidender Wichtigkeit, zumindest grundlegende Verfahren für die Cyberhygiene umzusetzen. Als Basis für den Schutz essentieller Infrastrukturen sollten Organisatio-

nen grundlegende Sicherheitsmaßnahmen implementieren – darunter regelmäßige Software- und Hardware-Updates, regelmäßige Passwortänderungen, die Verwaltung neuer Installationen, die Einschränkung von Kontenzugriff auf Administratorebene und die Sicherung von Daten.

Da viele Angriffe über vernetzte Geräte erfolgen, sind Schulungen und die Sensibilisierung der Mitarbeitenden für aktuelle Cyberbedrohungen unerlässlich. Nur so kann ein proaktives Umfeld und das nötige Bewusstsein geschaffen werden, um die Sicherheit der Betreiber wesentlicher Dienste in der EU zu stärken.

> **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.

Peer Reviews

Wie im Artikel 19 der NIS2-Richtlinie angegeben, wird die Kooperationsgruppe ein System von freiwilligen Peer Reviews errichten, mit dem die Mitgliedstaaten von gemeinsamen Erfahrungen lernen und die Cybersicherheit verbessern können. Die Peer Reviews umfassen verschiedene Themen, wie die Umsetzung der Maßnahmen bezüglich Cybersicherheitsrisikomanagement und der Berichtspflichten in den Ländern, die Wirksamkeit bei der Durchführung der Aufgaben der zuständigen Behörden und das Maß der gegenseitigen Unterstützung und des Austauschs von Informationen.

Die Peer Reviews können vor Ort oder virtuell durchgeführt werden – im Einklang mit dem Grundsatz der guten Zusammenarbeit und bei vollständiger Kooperation zwischen den Parteien. Nach dem Abschluss des Peer Reviews arbeiten die Sachverständigen für Cybersicherheit einen Berichtsentwurf aus, in dem die Ergebnisse sowie Empfehlungen für die Verbesserung der Cybersicherheit festgehalten werden. Die Berichte werden der Kooperationsgruppe und dem relevanten Cybersicherheitsnetzwerk vorgelegt und können auf Wunsch der dem Review unterliegenden Organisation öffentlich zugänglich gemacht werden.

Persönliche Haftung von Leitungsorganen

Mitgliedstaaten sollten Geldbußen und Strafen für Organisationen verhängen, die die in NIS2 definierten Maßnahmen nicht implementieren und teilen der Kommission bis 2025 diese Vorschriften und Maßnahmen mit. Neben Strafen für Organisationen sieht NIS2 in Artikel 20 aber auch eine persönliche Haftung für Leitungsorgane wie Unternehmensvorstände oder Führungskräfte von Organisationen vor, um die Erfüllung der Anforderungen für die Cybersicherheit durchzusetzen. Jede Nichteinhaltung kann zu verschiedensten Vollstreckungstiteln oder erheblichen Geldbußen führen.

Welche Organisationen sind von NIS2 betroffen?

Wie bereits erwähnt, sind von NIS2 mehr Organisationen betroffen als von der ursprünglichen NIS-Richtlinie. Einfach ausgedrückt, gilt die NIS2-Verordnung **vor allem für Einrichtungen, die wesentliche oder wichtige Dienste anbieten, und insbesondere jene mit mindestens 50 Mitarbeitenden bzw. einem Jahresumsatz ab 10 Millionen Euro.**

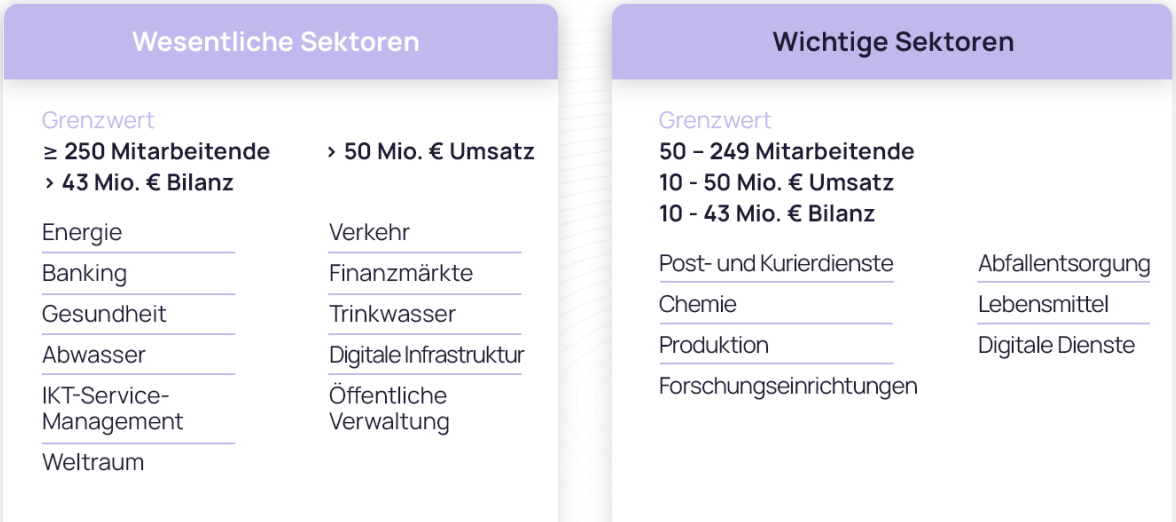
Um das Problem der unterschiedlichen Auffassungen in den Mitgliedstaaten im Hinblick darauf, was als Betreiber wesentlicher und wichtiger Dienste gilt, zu beseitigen und eine einheitliche Begrifflichkeit sicherzustellen, **teilt NIS2 die betreffenden Organisationen in zwei Gruppen auf: wesentliche Einrichtungen und wichtige Einrichtungen**. Außerdem erweitert sie den Geltungsbereich von NIS, indem neben anderen Sektoren auch Hersteller bestimmter Produkte und Anbieter digitaler Dienste einbezogen werden.

Nach den neuen Änderungen von NIS2 sind **wesentliche Einrichtungen** Unternehmen mit mindestens 250 Mitarbeitenden, einem Jahresumsatz ab 50 Millionen Euro und einer Jahresbilanzsumme von mindestens 43 Millionen Euro, die in den Sektoren Energie, Verkehr, Bankwesen, Finanzmärkte, Gesundheitswesen, Trinkwasser, Abwasser, digitale Infrastruktur, IKT-Dienste, öffentliche Verwaltung und Weltraum tätig sind. **Wichtige Einrichtungen** sind Organisationen mit weniger als 250 Mitarbeitenden, einem Jahresumsatz von 10 bis 50 Millionen Euro und einer Jahresbilanzsumme von weniger als 43 Millionen Euro in den Sektoren Post- und Kurierdienste, Abfallbewirtschaftung, chemische Stoffe, Lebensmittel, Fertigung, Anbieter digitaler Dienste und Forschung.

Wichtiger Hinweis: Organisationen, die die genannten Schwellenwerte für wichtige Sektoren überschreiten, aber trotzdem nicht unter die wesentlichen Einrichtungen fallen, müssen die Richtlinie gemäß den Vorgaben für wichtige Einrichtung erfüllen.

Für wesentliche und wichtige Einrichtungen gelten dieselben Cyber-Sicherheitsmaßnahmen und Meldepflichten. Unterschiede gibt es aber bei den Aufsichts- und Durchsetzungsregelungen – wesentliche Einrichtungen werden bei der Umsetzung überwacht, während wichtige Einrichtungen nur bei vorliegenden Nachweisen von Verstößen überprüft werden.

Auch wenn eine Organisation die Kriterien für eine wesentliche oder wichtige Einrichtung nicht erfüllt, kann sie sich trotzdem auf eigenen Wunsch nach NIS2 bewerten lassen, um ihr Cyber-Sicherheitssystem zu verbessern. Für die Registrierung müssen Organisationen folgende Informationen angeben: Name, Anschrift und Registrierungsnummer, Sektor, zu dem sie gemäß NIS2 gehören, Staat, Kontaktdetails sowie eine Liste der zugewiesenen IP-Adressen.



DORA und NIS2: Was sind die Unterschiede?

Als Reaktion auf die wachsenden Herausforderungen durch Cyberangriffe und zum Schutz wichtiger Systeme und der digitalen Infrastruktur in Europa hat die Europäische Kommission kürzlich zwei essentielle Rechtsvorschriften eingeführt: NIS2 – die in diesem Artikel behandelte Richtlinie – und DORA, den Digital Operational Resilience Act. Für beide gelten ähnliche Fristen: DORA wurde ursprünglich im Jahr 2020 vorgeschlagen und 2023 finalisiert. NIS2 wurde 2022 eingeführt und veröffentlicht und trat im Januar 2023 in Kraft.

Beide Verordnungen haben die Verbesserung der Cyberresilienz von Organisationen in Europa zum Ziel, richten sich aber an unterschiedliche Sektoren. NIS2 erweitert die NIS-Vorgängerrichtlinie und zielt auf die Standardisierung der Cybersicherheit und Governance für Betreiber von wesentlichen und wichtigen Diensten ab, wie Verkehr, Telekommunikation, Wasser- und Abfallwirtschaft, Rechenzentren, Bankwesen, öffentliche Verwaltung, Forschungsorganisationen, Post- und Kurierdienste und andere. **DORA ist hingegen eine neue Verordnung, mit der die Integrität digitaler Systeme in Finanzunternehmen** in Europa verbessert und die Erkennung, Behandlung und Meldung von IKT-spezifischen Risiken durch Organisationen harmonisiert werden soll.

Trotz ihrer unterschiedlichen Geltungsbereiche haben NIS2 und DORA ein gemeinsames Ziel: die Sicherheitsmaßnahmen von Organisationen in ganz Europa zu vereinheitlichen, die Integrität von Daten zu schützen und dem wachsenden Risiko von Sicherheitsverletzungen entgegenzuwirken.

Zeitplan zur Erfüllung der NIS2-Anforderungen

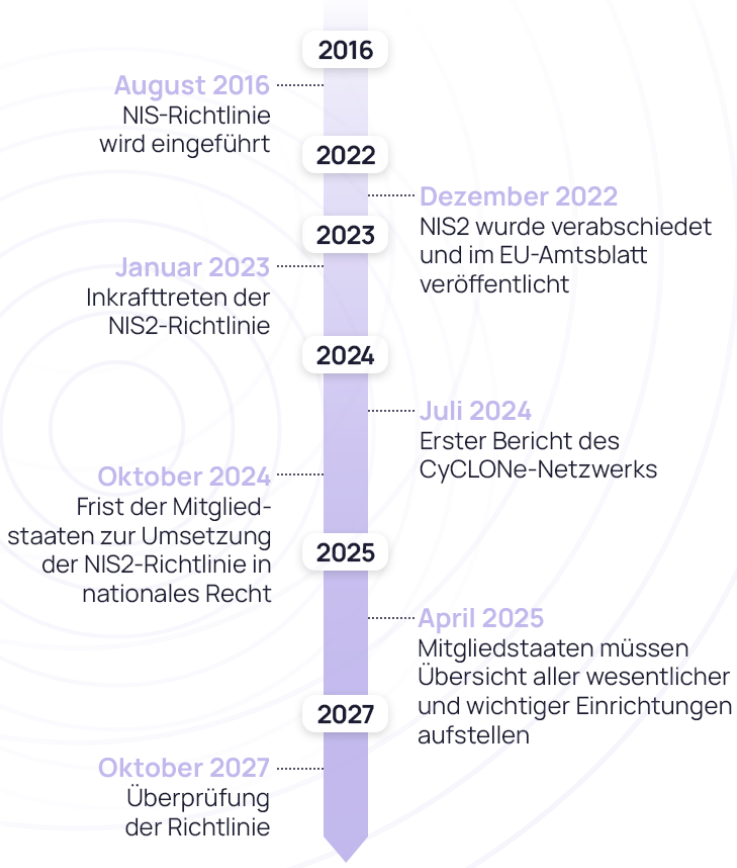
Im Juli 2016 haben das Europäische Parlament und der Rat der Europäischen Union die NIS-Richtlinie verabschiedet, um das Cyber-Sicherheitsniveau in der EU zu erhöhen und die Resilienz kritischer Infrastrukturen zu verbessern. Sie trat im August 2016 in Kraft, wobei den Mitgliedstaaten ein Zeitraum von 21 Monaten bis zum Mai 2018 gewährt wurde, um die Richtlinie in nationales Recht umzusetzen. Bis zu diesem Datum mussten Anbieter von wesentlichen Diensten und digitalen Diensten die vollständige Konformität mit den Cyber-Sicherheitsverordnungen und Meldepflichten der NIS-Richtlinie herstellen.

Durch die zunehmende Digitalisierung und die Häufung von Cyberangriffen wurde 2020 die Notwendigkeit einer robusteren Verordnung deutlich, um die Systeme und Daten von Betreibern wesentlicher Dienste zu schützen und den Geltungsbereich auf einige wichtige Sektoren auszuweiten. Deshalb legte die Europäische Kommission im Dezember 2020 einen Vorschlag für eine aktualisierte Version der ursprünglichen NIS-Richtlinie vor, die NIS2-Richtlinie. Nach einer einjährigen Überarbeitungs- und Verhandlungsphase wurde die NIS2-Richtlinie 2022 verabschiedet und am 27. Dezember 2022 im Amtsblatt veröffentlicht.

NIS2 trat offiziell am 16. Januar 2023 in Kraft. Die Mitgliedstaaten müssen die NIS2-Richtlinie bis zum 17. Oktober 2024 in nationales Recht umsetzen, um die Compliance sicherzustellen. Wenn die Anforderungen der NIS2-Richtlinie nicht innerhalb dieser Frist umgesetzt werden, können Bußgelder sowohl für Einzelpersonen als auch für Organisationen erhoben werden.

Bis zum 17. Juli 2024 und danach alle 18 Monate übermittelt das EU-CyCLONe-Netzwerk einen Bericht, in dem es seine Arbeit bewertet. Das CSIRT-Netzwerk erarbeitet bis zum 17. Januar 2025 ebenfalls einen Bericht, in dem der Fortschritt der Mitgliedstaaten bei der operativen Zusammenarbeit bewertet wird. Außerdem enthält der Bericht Schlussfolgerungen und Empfehlungen auf der Grundlage der Peer Reviews, die den gegenseitigen Erfahrungsaustausch, das Lernen und die Unterstützung in Compliance-Fragen fördern sollen. Bis zum 17. April 2025 erstellen die Mitgliedstaaten eine Liste von wesentlichen und wichtigen Einrichtungen, die unter die NIS2-Richtlinie fallen.

Die aktuelle NIS2-Richtlinie soll im Oktober 2027, drei Jahre nach ihrem Inkrafttreten, überprüft werden.



Folgen einer Nichteinhaltung

In der NIS2-Richtlinie sind grundlegende Sanktionen für Verstöße im Hinblick auf die Cyber-Sicherheitsmaßnahmen und Meldepflichten festgelegt. Diese Strafen für Organisationen, die die vereinbarten Fristen nicht einhalten, können unterschiedliche Formen haben, wie beispielsweise nicht-monetäre Rechtsmittel, Geldbußen und strafrechtliche Maßnahmen. Die exakte Art der Strafe variiert je nach Organisation und Abweichung zwischen der geforderten und der tatsächlichen Implementierung.

Nationale Aufsichtsbehörden können **nicht-monetäre Rechtsmittel** einsetzen, einschließlich Compliance-Verfügungen, verbindliche Anweisungen, Umsetzungsverordnungen für Sicherheitsprüfungen und Verfügungen für Bedrohungsmeldungen an die Kunden der Organisation.

Bei **Geldbußen** unterscheidet NIS2 zwischen wesentlichen und wichtigen Einrichtungen. Im Rahmen der neuen Verordnung können nationale Behörden wesentliche Einrichtungen mit einer maximalen Geldbuße in Höhe von 10 Millionen Euro oder 2 % des weltweiten Umsatzes belegen, je nachdem, welcher Betrag höher ist. Für wichtige Einrichtungen beträgt die maximale Höhe der Geldbußen 7 Millionen Euro oder 1,4 % des weltweiten Umsatzes, je nachdem, welcher Betrag höher ist.

Im Gegensatz zur Vorgängerrichtlinie verlagert NIS2 die Zuständigkeit für die Implementierung und Umsetzung von Sicherheitsmaßnahmen weg von der IT-Abteilung und **nimmt jetzt auch das Top-Management in die Verantwortung**. Die Mitgliedstaaten können nun C-Level-Manager haftbar machen, wenn aufgrund grober Fahrlässigkeit der Organisation ein Cybervorfall auftritt, wobei die Strafen variieren können. So können Compliance-Verstöße öffentlich gemacht oder die für den Verstoß verantwortliche(n) natürliche(n) oder juristische(n) Person(en) benannt werden. Handelt es sich um eine wesentliche Einrichtung, kann eine Person bei wiederholten Verstößen von allen Management-Positionen abgesetzt werden.

Nächste Schritte: So erfüllen Sie die NIS2-Richtlinie

Zwar gibt es eine relativ lange 24-Monats-Frist für die Umsetzung von NIS2, eine rechtzeitige Vorbereitung ist aber das A und O, um rechtzeitig vollständige NIS2-Compliance zu erreichen. Ausarbeitung einer Strategie, Abstimmung mit externen Lieferanten und Budgetplanung nehmen viel Zeit in Anspruch. Daher sollten Organisationen frühzeitig aktiv werden, um die Implementierung rechtzeitig und stressfrei über die Bühne zu bringen.

In der Implementierungsphase können Einrichtungen mit den folgenden Schritten Compliance erreichen:

1. Erörtern Sie gemeinsam mit dem Management und allen Beteiligten die Implementierungsstrategie und die Auswirkungen von NIS2 auf die tagtägliche Arbeit.

2. Stellen Sie sicher, dass alle Vorstandsmitglieder, die Manager, das IT-Team und die Mitarbeitenden, die die wesentlichen Dienste bereitstellen, die NIS2-Anforderungen kennen und verstehen.

3. Identifizieren Sie kritische Elemente und Prozesse, die für die Bereitstellung wesentlicher Dienste relevant sind, und führen Sie eine Lückenanalyse durch, um die Bereiche zu ermitteln, in denen die Cyber-Sicherheitsmaßnahmen die NIS2-Anforderungen noch nicht erfüllen.

4. Identifizieren Sie externe Lieferanten, die wesentliche Dienste bereitstellen, und ermitteln Sie deren potenzielle Schwachstellen.

5. Erarbeiten Sie einen Security-Awareness-Programm, das alle Ebenen der Organisation umfasst, um sicherzustellen, dass sowohl der Vorstand als auch die Mitarbeitenden über die aktuellen und bevorstehenden Änderungen bei den Arbeitsabläufen, über die Reporting-Anforderungen und über andere Cyber-Sicherheitsthemen im Bild sind.

6. Finden Sie Compliance-Partner, die Ihnen beim Erreichen der Compliance unterstützend oder beratend zur Seite stehen.

7. Weisen Sie das nötige Budget für die Umsetzung der NIS2-Anforderungen zu.

8. Führen Sie nach der Implementierung aller NIS2-Maßnahmen eine zweite Lückenanalyse durch, um sicherzustellen, dass Sie vollständige Compliance erreicht haben.

Wie SoSafe Sie auf dem Weg zur NIS2-Compliance unterstützen kann

Mit NIS2 wird die Vorgängerrichtlinie NIS erweitert und verbessert, so dass Anbieter von wesentlichen und wichtigen Diensten bestens auf die wachsenden Cybergefahren vorbereitet sind. Dazu müssen Organisationen einen ganzheitlichen Ansatz verfolgen, der die in NIS2 definierten Risikomanagement-Anforderungen, Meldepflichten und Reaktionspläne berücksichtigt.

Effektives Risikomanagement ist das Herzstück von NIS2. In den Artikeln 7, 9, 20 und 21 wird die Wichtigkeit von Schulungen sowohl für Leitungsorgane als auch für die Mitarbeitenden betont. Denn dadurch erhalten sie das Wissen und die Fertigkeiten, um Risiken zu identifizieren und Risikomanagementverfahren für die Cybersicherheit zu bewerten.

Das gamifizierte Awareness Training von SoSafe umfasst eine Vielzahl von Lernmodulen zu den verschiedenen Angriffsmethoden und Best Practices im Bereich der Cybersicherheit. Es befähigt Mitarbeitende, Bedrohungen zuverlässig zu erkennen und effizient zu bekämpfen. Die E-Learning-Plattform durchbricht außerdem Sprachbarrieren, indem Inhalte in mehr als 30 Sprachen bereitgestellt werden. Mit diesem multilingualen Ansatz begegnen wir Menschen mit den unterschiedlichsten Hintergründen und erfüllen gleichzeitig die rechtlichen Anforderungen von Ländern, die Weiterbildungen in der Muttersprache voraussetzen. Darüber hinaus bietet die Content-Management-Lösung von SoSafe die Möglichkeit, Ihren Mitarbeitenden alle Trainingsmodule und Sicherheitsrichtlinien – einschließlich Ihrer eigenen – an einem zentralen Ort zugänglich zu machen. Das steigert die Motivation Ihrer Mitarbeitenden und unterstützt nachhaltig die Compliance.

Effektives Awareness-Training geht jedoch weit über Trainingsmodule hinaus: Es muss eng in das tagtägliche Leben und die Kommunikation eingebunden werden. Unser Chatbot Sofie kann in Microsoft Teams integriert werden und ermöglicht so die direkte Verbindung mit Ihren Mitarbeitenden, um dringende Warnungen zeitnah zu übermitteln und Training-Nudges in wenigen Minuten zu senden.

Gemäß Artikel 11 der NIS2-Richtlinie müssen CSIRTs eine dynamische Analyse von Risiken und Sicherheitsvorfällen durchführen und eine Lagebeurteilung im Hinblick auf die Cybersicherheit vornehmen. Mit dem ISO-27001-konformen Risk & Reporting Cockpit von SoSafe können Sie systematische Analysen unter Berücksichtigung des menschlichen Faktors durchführen und behalten den Fortschritt Ihres Awareness-Programms immer im Blick. Zudem bietet es Zugriff auf detaillierte Analysen und wichtige Kennzahlen zu den menschlichen Risikofaktoren innerhalb Ihrer Organisation. Für das zeitnahe Reporting bieten wir mit dem Phishing-Meldebutton und dem integrierten Feature namens Phish Assist ein nützliches Tool, mit dem Mitarbeitende Sicherheitsvorfälle schnell und unkompliziert melden können und so die Früherkennung und das zeitnahe Reporting von Bedrohungen unterstützen.

Durch die Einhaltung der NIS2-Anforderungen und die Bereitstellung wichtiger Ressourcen und Schulungen stellen Sie Ihre Compliance sicher und **stärken zudem die Verteidigungslinie Ihrer Organisation** gegen Cyberbedrohungen. So können Sie Unterbrechungen des Geschäftsbetriebs vermeiden und Ihre Organisation effektiv schützen.

Stärken Sie Ihre Sicherheitskultur – einfach und effektiv

Mit seiner Awareness-Plattform hilft SoSafe Organisationen, ihre Sicherheitskultur zu stärken und menschliche Risikofaktoren zu minimieren. Die Plattform bietet motivierende Lernerfahrungen und smarte Angriffssimulationen, die Mitarbeitende dazu befähigen, Cyberbedrohungen zu erkennen und aktiv abzuwehren – alles basierend auf verhaltenspsychologischen Erkenntnissen, die das Lernen spannender und effektiver gestalten. Anhand umfassender Analytics werden Verhaltensänderungen gemessen und Schwachstellen aufgedeckt, sodass Cyberbedrohungen proaktiv vorgebeugt werden kann. Die SoSafe Plattform ist im Handumdrehen eingerichtet und wächst mit Ihrem Unternehmen, um so sicheres Verhalten bei den Mitarbeitenden nachhaltig zu festigen.

TEACH — Motivierendes Micro-Learning

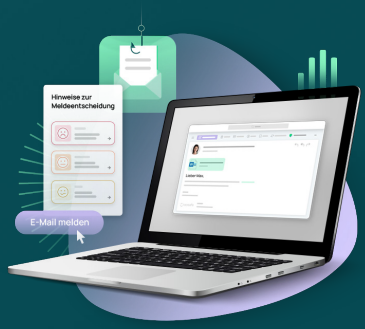
Eine verhaltenspsychologisch fundierte E-Learning-Plattform, mit der Lernen Spaß macht. Dynamische und wirkungsvolle Lernerfahrungen auf verschiedenen Kanälen helfen Ihnen, Ihre Abwehr gegen Cyberbedrohungen zu stärken, volle Compliance zu erzielen und mühelos sichere Verhaltensweisen aufzubauen.

- Storybasierte Micro-Lerninhalte mit Gamification-Elementen motivieren und fördern nachhaltig sichere Verhaltensweisen
- Ausgewählte, strukturierte Inhalte, die sich einfach skalieren lassen
- Benutzerfreundliche Customization- und Content-Management-Optionen, auf Ihr Unternehmen abgestimmt

TRANSFER — Smart Angriffssimulationen

Zielgerichtete Phishing-Simulationen, um sichere Verhaltensweisen bei Ihren Mitarbeitenden zu fördern. Mit regelmäßigen, automatisierten Spear-Phishing-Simulationen befähigen Sie Ihre Mitarbeitenden, Cyberattacken zu erkennen und Security Awareness zu einem festen Bestandteil ihres Arbeitsalltags zu machen. Reduzieren Sie Ihr Cyberrisiko und Ihre Reaktionszeit im Falle eines Angriffs.

- Personalisierbare, realistische Simulationen von Cyberangriffen
- Kontextbasierte Lernseiten, die sichere Verhaltensweisen des Teams festigen
- Unmittelbares Reporting mit nur einem Klick dank Phishing-Meldebutton



ACT — Strategisches Risk Monitoring

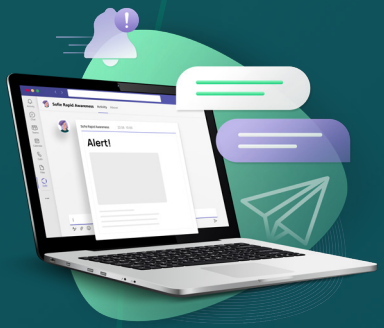
Behalten Sie menschliche Risikofaktoren mit unserer Lösung immer im Blick und schützen Sie Ihre Organisation vor kostspieligen Sicherheitsvorfällen. Mit umfangreichen Daten und verhaltenspsychologisch fundierten Insights können Sie mögliche Schwachstellen beheben. Sie erhalten zudem ein ganzheitliches Bild über das Verhalten Ihrer Mitarbeitenden und den Erfolg Ihres Security-Awareness-Programms und können dadurch fundierte strategische Entscheidungen treffen.

- Aufschlussreiche Insights durch kontextuelle Daten, wie technische KPIs und verhaltensbasierte Kennzahlen
- Branchenspezifische Benchmarks und Handlungsempfehlungen für den Ernstfall
- Auf Audits nach ISO/IEC 27001 ausgelegt und 100 Prozent DSGVO-konform

CONNECT — Sofie Rapid Awareness

Cyberkriminelle entwickeln ihre Methoden schneller weiter als je zuvor, aber Sie können das auch. Rapid Awareness ermöglicht es Ihnen, Ihre Mitarbeitenden schnell und einfach in MS Teams zu erreichen. Halten Sie durch effektives Micro-Learning mit Cyberbedrohungen Schritt, versorgen Sie Ihr Team mit Alerts zu den neuesten Angriffsmaschen und machen Sie Ihre Mitarbeitenden zu Ihrer stärksten Verteidigungslinie.

- Erreichen Sie Ihre Mitarbeitenden direkt in MS Teams
- Sparen Sie Zeit und kommunizieren Sie mit Leichtigkeit
- Senden Sie kurze und leicht verständliche Alerts an Ihre Mitarbeitenden
- Verfolgen Sie, wie viele Mitarbeitende die Alerts gesehen haben



sosafe

SoSafe GmbH
Lichtstrasse 25a
50825 Köln

info@sosafe.de
www.sosafe-awareness.com/de
+49 221 65083800