sosafe

NIS-2-Guide: Roadmap zum Einhalten von Security-Training-Verpflichtungen

Praktische Schritte, realistische Zeitpläne und Auditbereitschaft

Übersicht

Einleitung 3

NIS-2 navigieren: Behörden, Einrichtungen und Zeitrahmen 4

NIS-2-Compliance in der DACH-Region 6

Die wichtigsten Vorgaben von NIS-2, die keine Organisation ignorieren darf 9

Organisationen mithilfe der Mitarbeitenden schützen 11

Entscheidungsfaktoren bei der Auswahl einer Trainings- und Awareness-Lösung 14

An regulatorische Anforderungen angepasste Lösungen von SoSafe 15

In 90 Tagen auf der Schnellspur zur Awareness-Compliance 18

Machen Sie den nächsten Schritt, um sicher aufgestellt zu sein 19

Einleitung

Die Pandemie hat gezeigt, wie schnell digitale Systeme zusammenbrechen und wie anfällig kritische Services sein können. Die Reaktion von Europa war NIS-2, **eine stärkere Richtlinie**, die diejenige von 2016 ersetzt und auf eine klarere Verantwortlichkeit und größere Resilienz abzielt.

Die neue Richtlinie hat einen breiter angelegten Umfang, der **mehr Sektoren umfasst**, und sie kommt genau zur richtigen Zeit. Im letzten Jahr haben neun von zehn Organisationen einen Cybersicherheitsvorfall von **genau der Art erlebt, die NIS-2 verhindern soll**, und wie eine Umfrage von 2024 ergab, war fast die Hälfte von ihnen mehr als einmal betroffen. Diese Zahlen zeigen deutlich, wie überfällig strengere Regelungen sind.

In diesem Kontext kommt NIS-2 ins Spiel, erhöht die Rechenschaftspflicht, erweitert ihren Umfang und erfordert Nachweise für Resilienz. Doch 53 % der IT-Führungskräfte fragen sich noch immer, ob NIS-2 ausreicht. Die Anforderungen der Richtlinie sind einfach: Zeigen Sie, dass Sie vorbereitet sind.

NIS-2 wird heute mehr als **180.000 Organisationen in ganz Europa** betreffen, von Gesundheits- und Transportwesen bis hin zur Fertigung und der breiteren Lieferkette. SoSafe unterstützt diese Sektoren schon seit langem in genau dem Bereich der Cybersicherheit, der nun kritisch geprüft wird: **Awareness und Training**. 30 Prozent der IT-Führungskräfte nennen dies als den **herausforderndsten Aspekt der NIS-2-Compliance**, auch wenn die Schwierigkeit in der Praxis oft darin liegt, wie das Ganze angegangen wird.

NIS-2 fragt nicht danach, ob Trainings vorhanden sind. Sie fragt, ob sie funktionieren, die richtigen Personen erreichen und nachgewiesen werden können. **SoSafe hilft Organisationen, diesen Standard zu erfüllen – mit Programmen, die für die Compliance konzipiert wurden, aber darauf ausgerichtet sind, Verhaltensweisen von innen heraus zu ändern.**

Dieser Guide beschreibt, was NIS-2 von Organisationen und Unternehmen beim Aufbau einer Sicherheitskultur erfordert, und zeigt, wie sie sich **mit Nachweisen vorbereiten können**, die Regulierungsbehörden überzeugen und Vertrauen aufbauen.

NIS-2 navigieren: Behörden, Einrichtungen und Zeitrahmen

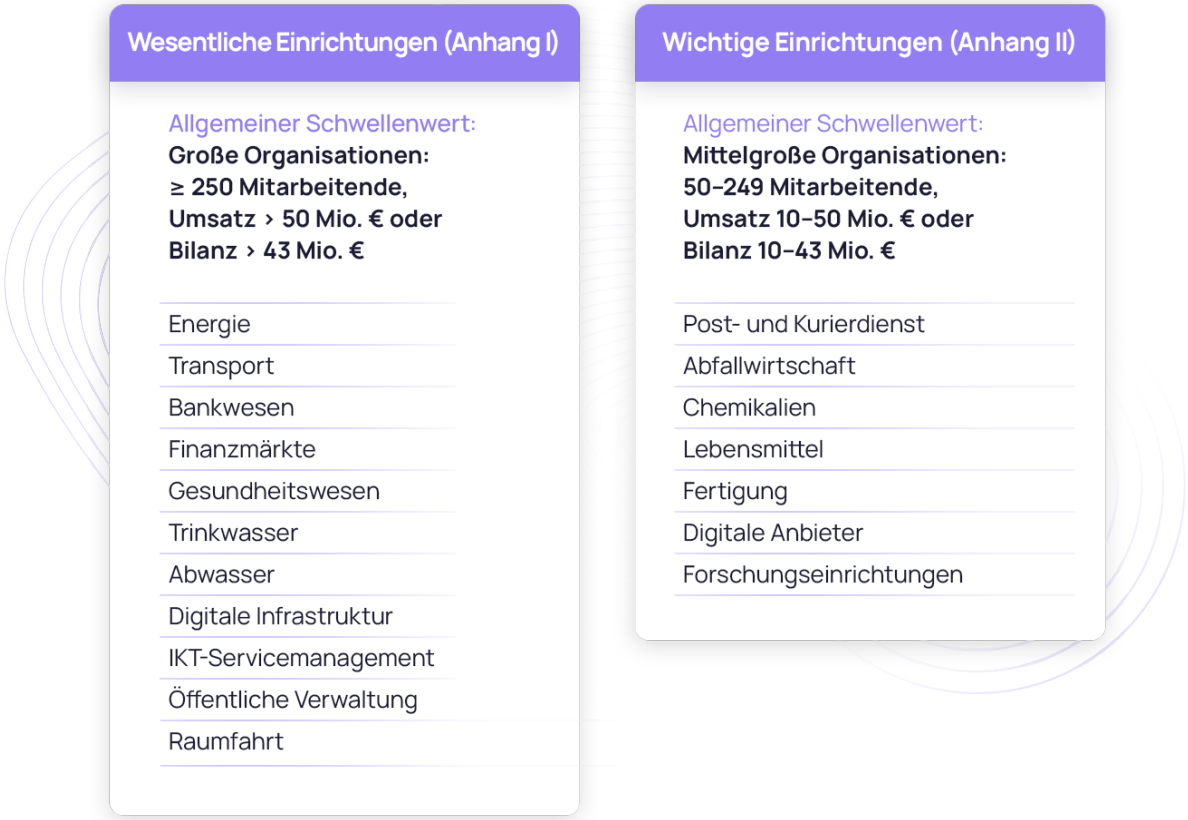
Hinter NIS-2 steht ein Framework, das klare Regeln mit praktischem Support kombiniert und Organisationen sowohl Verpflichtungen gibt, die sie einhalten müssen, als auch Systeme, auf die sie sich verlassen können.

Das **Regelbuch hat drei Ebenen**: Die Direktive legt die Regeln fest, die Regulierung spezifiziert sie für den digitalen Sektor und die ENISA-Anweisungen zeigen, wie sie angewendet werden. Andere Sektoren können die Anweisungen als empfehlenswerte Praxis berücksichtigen, doch nationale Regeln haben Priorität.

Zusätzlich schafft NIS-2 ein **koordiniertes Verteidigungssystem**, das Organisationen einsetzen können, wenn Vorfälle eskalieren. Nationale CSIRTs übernehmen die erste Reaktion, während EU-CyCLONe und die NIS-Kooperationsgruppe die grenzüberschreitende Koordination und gemeinsame Leitung übernehmen. Zudem führt NIS-2 eine EU-weite Schwachstellendatenbank ein, sodass Organisationen Schwachstellen frühzeitig registrieren können.

NIS-2 betrifft hauptsächlich **mittlere und große Organisationen in kritischen Sektoren**. Kleinstunternehmen und kleine Unternehmen sind ausgeschlossen, sofern ein Mitgliedstaat nichts Gegenteiliges beschließt. Für einige Einrichtungen wie Vertrauensdiensteanbieter, DNS-/TLD-Registrierungen und zentrale Verwaltungsbehörden gilt NIS-2 immer, unabhängig von ihrer Größe.

Grenzüberschreitende Unternehmen sind gegenüber ihrem Hauptsitz in der EU und nicht gegenüber mehreren nationalen Behörden rechenschaftspflichtig, aber Tochtergesellschaften können dennoch eingeschlossen werden, da **die Schwellenwerte auf Konzernebene gelten**. Jeder Mitgliedstaat muss eine Liste von wesentlichen und wichtigen Einrichtungen führen und Unternehmen müssen ihren Status national überprüfen.



Die betroffenen Unternehmen müssen mit einer strengeren Aufsicht rechnen. Behörden können **Audits und Inspektionen** durchführen, Korrekturmaßnahmen fordern und Strafen auferlegen. **Bußgelder können hoch sein** und bis zu 10 Millionen Euro oder 2 % des globalen Umsatzes für wesentliche Einrichtungen sowie 7 Millionen Euro oder 1,4 % für wichtige Einrichtungen betragen.

Die Umsetzungsfristen sind auf EU-Ebene festgelegt, doch **die nationalen Fortschritte variieren**, sodass es für Organisationen sehr wichtig ist, die lokalen Entwicklungen zu verfolgen. Die Durchsetzung steht kurz bevor und Organisationen haben keine Zeit zu verlieren.

NIS-2-Compliance in der DACH-Region

In der DACH-Region verfügen fast 40 Prozent der Einrichtungen der kritischen Infrastruktur noch über kein formelles Awareness-Programm – ähnlich sieht es laut ENISA im öffentlichen Sektor aus. Zu den Bereichen, in denen Sicherheitsbeauftragte in Deutschland besonders starke Anpassungen vornehmen müssen, gehören das Überarbeiten des Technologie-Stack und der Cyber-Sicherheitslösungen sowie das Training von Mitarbeitenden und der Führungsebene.

Anwendungsbereich und betroffene Sektoren

Die NIS-2-Richtlinie erweitert den Anwendungsbereich in Deutschland, Österreich und der Schweiz deutlich. In Deutschland werden ab Ende 2025 bzw. Anfang 2026 rund **30.000 Organisationen** betroffen sein – viermal so viele wie bisher. Dazu zählen vor allem Einrichtungen in den Bereichen Energie, Verkehr, Gesundheit (über 1.900 Krankenhäuser), Finanz- und Versicherungswesen, digitale Infrastruktur, öffentliche Verwaltung sowie Produktion und Logistik. Die Trinkwasser- und Abwassersektoren sollen zur Implementierung als ein Sektor gelten.

In Österreich und der Schweiz gelten ähnliche sektorspezifische Regelungen, wobei die Umsetzung in der Schweiz aufgrund der Nicht-EU-Mitgliedschaft spezifisch angepasst wird. In Österreich geht man von rund **4.000 Organisationen** aus, in der Schweiz von etwa **1.200**. Auch KMU ab 50 Mitarbeitenden oder 10 Mio. Euro Jahresumsatz fallen unter die Vorgaben, sofern sie kritische Leistungen erbringen.

Rahmenwerke – Standards zum Nachweis der Compliance

Zur Erfüllung der NIS-2-Anforderungen werden in der DACH-Region vor allem international anerkannte Standards genutzt. In Deutschland gilt **ISO/IEC 27001** als zentraler Prüfmaßstab, ergänzt durch **IEC 62443** für industrielle Steuerungs- und Automatisierungssysteme. Unternehmen orientieren sich zudem an den **ENISA-Leitlinien** sowie an Vorgaben nationaler Behörden wie dem **IT-Grundschutz-Kompendium des BSI**.

In Österreich erfolgt die Umsetzung über das **Netz- und Informationssystemsicherheitsgesetz (NISG)**, das die EU-Richtlinie in nationales Recht überführt und dabei ISO/IEC 27001, ISO/IEC 22301 sowie branchenspezifische Mindeststandards empfiehlt.

In der Schweiz, die nicht direkt an NIS-2 gebunden ist, greifen Unternehmen auf das Informationssicherheitsgesetz (ISG), das **Nationale Zentrum für Cybersicherheit (NCSC)** sowie internationale Standards wie ISO/IEC 27001 zurück, um Kompatibilität zu gewährleisten.

Meldepflichten und Fristen

Unternehmen in der DACH-Region sind verpflichtet, sicherheitsrelevante Vorfälle innerhalb enger Fristen zu melden: eine erste Meldung spätestens **24 Stunden** nach Entdeckung des Zwischenfalls, eine erste Bewertung mit technischen Details **innerhalb von 72 Stunden** sowie einen abschließenden Bericht **innerhalb von einem Monat.**

Diese Pflicht gilt für alle wesentlichen Störungen der Netz- und Informationssicherheit, wobei insbesondere **Dienstleistungsunterbrechungen, erhebliche Datenverluste oder Gefährdungen der öffentlichen Sicherheit** erfasst werden.

In Deutschland präzisiert das BSI, dass auch Vorfälle mit **erheblicher Beeinträchtigung der Versorgungssicherheit oder Verfügbarkeit kritischer Prozesse** meldepflichtig sind. In Österreich konkretisiert das NISG vergleichbare Schwellenwerte, in der Schweiz werden die Vorgaben über das ISG und Meldestellen beim NCSC geregelt.

Registrierungspflichten und zuständige Stellen

Betroffene Organisationen sind verpflichtet, sich bei ihren jeweils zuständigen nationalen Behörden zu registrieren. In Deutschland erfolgt die Registrierung beim **BSI**, das eine führende Rolle übernommen hat, oder über zuständige **CERT-Stellen**.

In Österreich übernimmt das **Bundesministerium für Finanzen (BMF)** als nationale Behörde die Koordination nach dem NISG, unterstützt durch die nationale Meldestelle beim GovCERT Austria. In der Schweiz liegt die Verantwortung beim **Nationalen Zentrum für Cybersicherheit (NCSC)**, das auch als zentrale Kontaktstelle dient.

Die Registrierungsfristen orientieren sich am Zeitpunkt des Inkrafttretens: In Deutschland wird die Registrierung voraussichtlich ab Ende 2025 oder Anfang 2026 verpflichtend sein, in Österreich innerhalb von drei Monaten nach Inkrafttreten der überarbeiteten NISG-Novelle. In der Schweiz gelten die Pflichten gemäß **Informationssicherheitsgesetz (ISG)** bereits seit 2023, wobei registrierungspflichtige Betreiber ihre Daten unverzüglich bereitstellen und Änderungen zeitnah nachmelden müssen.

Durchsetzung und Folgen bei Nicht-Einhaltung

Die NIS-2-Umsetzung in Deutschland sieht strenge Sanktionen vor: Bußgelder können bis zu **20 Millionen Euro oder 2 % des weltweiten Jahresumsatzes** betragen, je nachdem, welcher Wert höher ist. Zusätzlich drohen Maßnahmen wie behördliche Auflagen, zeitweise Untersagung des Geschäftsbetriebs oder die persönliche Haftung von Geschäftsführungs- und Vorstandsmitgliedern. Das BSI erhält erweiterte Befugnisse zur **Überwachung, Kontrolle und Anordnung von Sicherheitsmaßnahmen.**

In Österreich sind vergleichbare Sanktionen im **NISG** vorgesehen, darunter Geldstrafen bis zu **10 Millionen Euro oder 2 % des Jahresumsatzes**, ergänzt durch behördliche Anordnungen und strafrechtliche Schritte bei grober Fahrlässigkeit.

In der Schweiz regelt das **Informationssicherheitsgesetz (ISG)** die Sanktionen: Verantwortliche Organisationen können mit Geldstrafen bis **250.000 CHF**, bei Vorsatz und schweren Verstößen auch mit strafrechtlichen Konsequenzen belegt werden.

Besonders hervorgehoben wird in allen drei Ländern die **Verantwortung der Führungsebene**, die im Fall von Verstößen ausdrücklich zur persönlichen Haftung herangezogen werden kann.

Die wichtigsten Vorgaben von NIS-2, die keine Organisation ignorieren darf

Auch wenn sich die nationalen Umsetzungen unterscheiden, sind die Verpflichtungen in ganz Europa gleich. Von Organisationen wird erwartet, dass sie **angemessene**, dem Stand der Technik entsprechende Kontrollen einrichten, ihre Wirksamkeit nachweisen und Schwachstellen unverzüglich beheben (Art. 21).

Um gleiche Voraussetzungen für alle zu schaffen, legt NIS-2 **10 wesentliche Elemente** fest, die jede Organisation in die Praxis umsetzen muss.

Kernanforderungen von NIS-2 (Art. 21(2))

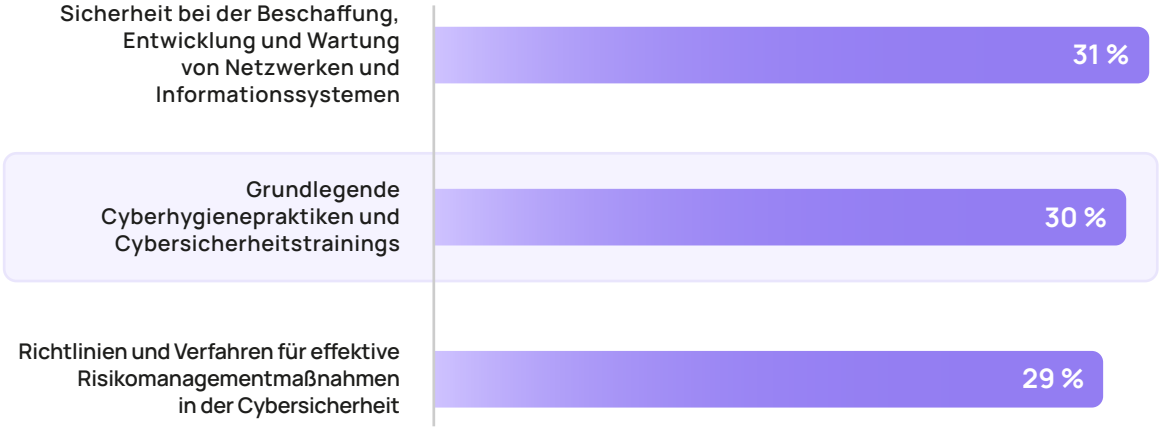
1. Risikoanalyse und Sicherheitsrichtlinie.
2. Umgang mit Vorfällen.
3. Geschäftskontinuität und Krisenmanagement (Backups, Wiederherstellung).
4. Lieferkettensicherheit für direkte Zulieferer und Dienstleister.
5. Sichere Akquisition, Entwicklung und Wartung (mit Behandlung und Offenlegung von Schwachstellen).
6. Testen der Wirksamkeit von Maßnahmen.
7. Grundlegende Cyberhygiene und regelmäßige Cybersicherheitstrainings.
8. Kryptografie und Verschlüsselung, wo angemessen.
9. HR-Sicherheit, Zugriffskontrollen und Bestandsverwaltung.
10. Starke Authentifizierung und sichere Kommunikation.

Die Meldung von Vorfällen unterliegt den strengsten Fristen: eine Frühwarnung innerhalb von 24 Stunden, eine Benachrichtigung innerhalb von 72 Stunden und eine Abschluss- oder Fortschrittsmeldung innerhalb eines Monats. Klar festgelegte Rollen, eine zuverlässige Dokumentation und eine reibungslose Kommunikation sind entscheidend, um dies zu ermöglichen (Art. 23).

Die Verantwortlichkeit erstreckt sich auch auf die **Lieferkette**. Organisationen müssen Schwachstellen und Entwicklungspraktiken von Zulieferern bewerten und dabei Risikobewertungen auf EU-Ebene berücksichtigen. (Art. 22). Die **Direktive legt die Grundprinzipien fest**: Governance an der Spitze, Resilienz über Systeme und Lieferanten hinweg und Rechenschaftspflicht durch schnelles, transparentes Reporting. Außerdem legt sie einen klaren Fokus auf Training und Awareness.

Zusammengenommen sollen diese Anforderungen die Cybersicherheit in Europa auf einen gemeinsamen Standard heben. Dennoch bleiben viele Verpflichtungen nach wie vor **unzureichend verstanden**, wodurch die Compliance zu einem beweglichen Ziel wird. 3 von 10 IT-Führungskräften nennen Cybersicherheitstrainings als den schwierigsten Teil der NIS2-Compliance und stufen sie als die zweitgrößte Herausforderung insgesamt ein.

Die 3 größten Compliance-Herausforderungen für IT-Führungskräfte unter NIS-2



Quelle: Zscaler, 2024

Die Direktive setzt den Faktor Mensch auf eine Ebene mit technischen Kontrollen (Erwägungsgrund 78) und macht die Awareness zu einer messbaren Verpflichtung. Mitarbeitende benötigen **Trainings, die reale Bedrohungen wie Phishing und Social Engineering widerspiegeln** (Erwägungsgrund 89). Auch die Führungsetage ist davon nicht ausgenommen. **Vorstände** müssen das Programm überwachen und selbst Trainings durchlaufen und die persönliche Haftung für Compliance-Verstöße übernehmen (Art. 20).

> "**Artikel 20(2).** Die Mitgliedstaaten stellen sicher, dass die Mitglieder der Leitungsorgane wesentlicher und wichtiger Einrichtungen an Schulungen teilnehmen müssen, und fordern wesentliche und wichtige Einrichtungen auf, allen Mitarbeitern regelmäßig entsprechende Schulungen anzubieten, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste zu erwerben."

Die Direktive kodifiziert technische Standards, erkennt jedoch auch an, dass Menschen, ihr Urteilsvermögen, ihr Training und ihre Verantwortlichkeit weiterhin entscheidend sind.

Organisationen mithilfe der Mitarbeitenden schützen

Der Faktor Mensch spielt bei Cybersicherheitsrisiken schon immer eine Rolle. 2024 waren bei nahezu sieben von zehn Sicherheitsverletzungen (68 %) auf die eine oder andere Weise menschliche Fehler beteiligt. Security-Verantwortliche erkennen das Muster wieder: Vier von zehn glauben, dass ihr nächster großer Vorfall mit einer menschlichen Schwachstelle beginnen wird. Noch größer ist diese Sorge in Spanien (53 %), Frankreich (45 %) und der DACH-Region (44 %).

Auch Angreifern ist dies bewusst. Sie müssen sich keinen Zugang erzwingen, wenn Überzeugungsarbeit genauso gut funktioniert. Autorität, Dringlichkeit und fehlgeleitetes Vertrauen sind ihre bevorzugten Hebel. In einem Moment von Stress oder Ablenkung können selbst gut geschulte Mitarbeitende kalt erwischt werden.

Sicherheitsverletzungen kosten mittlerweile Millionen – durchschnittlich 4,4 Millionen Euro pro Vorfall, wobei Sektoren wie das Gesundheitswesen noch größere Verluste erleben. Regulierungsbehörden beobachten diesen Trend ebenfalls und haben daher nun Awareness und Training gesetzlich festgeschrieben.

Dies führt dazu, dass Compliance heutzutage anders aussieht. Teilnahmezettel und Kurse, bei denen man Kästchen abhakt, reichen nicht mehr aus. Regulierungsbehörden erwarten sichtbare Zeichen für Verhaltensänderungen.

NIS-2 macht Awareness und Cyberhygiene zu einem Bestandteil der Compliance selbst, einschließlich ENISA-Fortschrittsberichten alle zwei Jahre (Art. 18). Ihre Anweisungen verwandeln breit angelegte Regeln in praktische Schritte, die Organisationen umsetzen und nachweisen können, wie das nachstehende Beispiel zeigt.

"**8.1.2.** Für die Zwecke von Nummer 8.1.1 bieten die betreffenden Einrichtungen ihren Mitarbeitenden, den Mitgliedern ihrer Leitungsorgane sowie – soweit angemessen – direkten Anbietern und Diensteanbietern gemäß Nummer 5.1.4 ein Sensibilisierungsprogramm an, das

a) zeitlich so geplant ist, dass die Maßnahmen wiederholt werden und neue Mitarbeitende erreichen;

b) mit dem Konzept für die Sicherheit von Netz- und Informationssystemen, den themenspezifischen Konzepten und den einschlägigen Verfahren für die Sicherheit von Netz- und Informationssystemen im Einklang steht;

c) einschlägige Cyberbedrohungen, bestehende Risikomanagementmaßnahmen im Bereich der Cybersicherheit, Kontaktstellen und Ressourcen für zusätzliche Informationen und Beratung zu Cybersicherheitsfragen sowie Verfahren im Bereich der Cyberhygiene für Nutzer abdeckt."

Quelle: ENISA

Die Richtlinie behandelt Menschen faktisch als Sicherheitsrisiko, das kontrolliert werden kann. Die Dokumentation zeigt, wie dies erfolgen soll:

Awareness für alle	Wiederkehrende Programme für Mitarbeitende, Management und gegebenenfalls Zulieferer, abgestimmt auf die Sicherheitsrichtlinien.
Rollenspezifische Trainings	Gezielte, praktische Trainings für Admins, Entwicklungsteams und andere Hochrisikorollen, bei Bedarf mit Zertifizierungen.
Grundlegende Cyberhygiene	Starke Authentifizierungs-, Phishing- und Social-Engineering-Awareness, sicheres Surfen, Backups, Updates und sicheres Remote Work.
Tests und Updates	Quiz, Übungen oder Feedback zum Messen der Wirkung mit jährlicher Auffrischung, um mit sich weiterentwickelnden Bedrohungen Schritt zu halten.
Tracking und Nachweise	Protokolle, Metriken, Zertifikate und Anwesenheitsnachweise, um die Compliance nachzuweisen und den Abschluss zu belegen.

Zusammengenommen zeigen diese Schritte auf, wie Compliance in der Praxis aussieht. Gleichzeitig sind sie auch der Punkt, an dem viele Organisationen ins Stolpern geraten.

Das Entwerfen, Bereitstellen und Nachweisen von **Programmen in großem Maßstab** erfordert Struktur, Fachwissen und zuverlässige Daten. Ohne das ist die Compliance unerreichbar, und damit auch die Resilienz gegen Angriffe, die nach wie vor meist bei Menschen beginnen. Ein vertrauenswürdiger Partner kann diese Lücke schließen und sowohl die Kapazität als auch die Nachweise liefern, die Regulierungsbehörden heutzutage erwarten.

Entscheidungsfaktoren bei der Auswahl einer Trainings- und Awareness-Lösung

Wenn Sie nach externer Unterstützung suchen, ist es enorm wichtig, eine gute Wahl zu treffen. Die Compliance beansprucht Ihre Zeit- und Geldbudgets, und welche Ergebnisse Sie erzielen, hängt von dem Partner ab, den Sie wählen. Die folgenden Fragen können Sie bei der Entscheidung unterstützen.

Wichtige Fragen, die Sie Anbietern zur NIS-2-Human-Risk-Compliance stellen sollten:

- [ ] Ist das Training in **jeder von Ihrem Personal benötigten Sprache** verfügbar und erfolgt es **kontinuierlich**, sodass auch neue Angestellte immer abgedeckt sind?
- [ ] Können auch **nicht im Büro (oder im Außendienst) tätige Mitarbeitende** auf das Training zugreifen? Sind Optionen wie persönliche Sitzungen vor Ort, Druckmaterialien oder geteilte Geräte verfügbar?
- [ ] Wie werden **Vorfälle** von Nutzenden formell eskaliert?
- [ ] Kann der Anbieter Nachweise in **von Auditoren anerkannten Formaten wie ISO** bereitstellen und diese unkompliziert exportieren?
- [ ] Kann das Tool Trainings über **Kanäle bereitstellen, die das Personal bereits verwendet**?
- [ ] Wo werden Ihre **Daten** gespeichert, welche Gesetze gelten und wie lang werden die Daten aufbewahrt?
- [ ] Welche **Integrationen für Unternehmenssoftware** wie Teams, Outlook, Entra ID oder LMS/LXP werden nativ unterstützt und wie werden sie gepflegt?
- [ ] Können Trainings auf **Rollen, Funktionen und Risikoprofile** in Ihrer Organisation zugeschnitten werden?
- [ ] Wie wird die **Effektivität** des Trainings in der Praxis überprüft und welche **Verhaltensmetriken** werden im Laufe der Zeit getrackt (z. B. Klickraten, Melderaten, Risikogruppen)?
- [ ] Wie wird sichergestellt, dass Training und Reporting sich bei sich ändernden Risiken und Gesetzen **weiterentwickeln**?

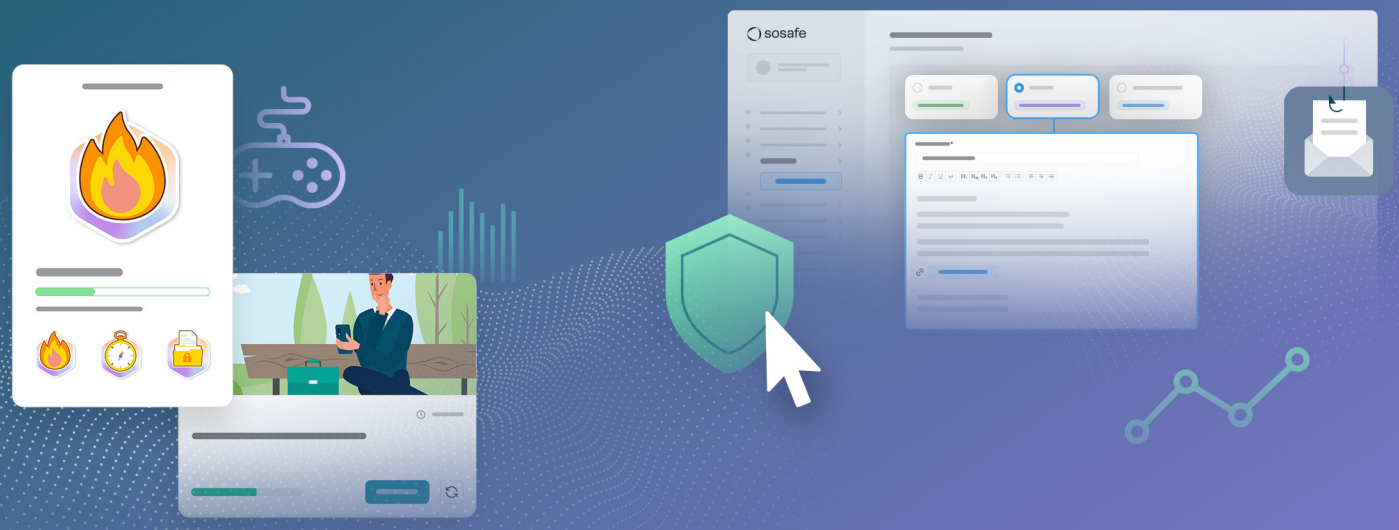
An regulatorische Anforderungen angepasste Lösungen von SoSafe

In Europa führen die meisten Unternehmen bereits Cybersicherheitstrainings durch, doch viele davon sind veraltet, als pauschale Einheitslösung gestaltet und liefern keinen Nachweis dafür, dass sie tatsächlich funktionieren. Mit NIS-2 ist das nicht mehr akzeptabel. Die Regulierungsbehörden verlangen Nachweise dafür, dass Mitarbeitende im gesamten Unternehmen, von Führungskräften bis hin zu außerhalb des Büros tätigem Personal, Trainings erhalten, die zu ihren Aufgaben passen, ihr Verhalten mit der Zeit verbessern und Ergebnisse erzielen, die einem Audit standhalten können. Für die meisten Teams kommen traditionelle Awareness-Programme an diesem Punkt an ihre Grenzen. Um diese Lücke zu schließen, braucht es **ein System, das gleichermaßen für Compliance und Resilienz konzipiert ist**.

SoSafe wurde genau für diese Realität entwickelt. Seine Programme **machen Awareness zu einem kontinuierlichen Prozess**, mit kurzen Sitzungen in mehr als 30 Sprachen und dedizierten Modulen für Vorstand und Führungskräfte.

Phishing-Simulationen testen die Bereitschaft unter realen Bedingungen und generieren solide Daten dazu, wie das Personal reagiert. Gleichzeitig leitet der **Phishing-Meldebutton** Vorfälle direkt in Sicherheitsworkflows.

Artikel 20 (2)	Personalisiertes Lernen
Artikel 21(2)(g)	Phishing-Simulationen



Hinter den Kulissen sammelt das **Human Risk OS** Analytics aus der gesamten Organisation und kombiniert Verhaltensdaten mit technischen Signalen, um nicht nur zu zeigen, wer ein Training absolviert hat, sondern auch, ob die Organisation tatsächlich Risiken reduziert. **ISO- und NIS-2-konforme Reports** werden automatisch erstellt und die Daten können über eine API in Drittanbietersysteme exportiert werden, sodass keine hektischen Vorbereitungen mehr erforderlich sind, wenn Regulierungsbehörden anfragen.

Artikel 21 (2) (f)	Human Risk OS

Was SoSafe von anderen unterscheidet, ist, wie sehr **Awareness zum Teil der alltäglichen Arbeitsumgebung wird**. Sie geschieht nicht außerhalb der Arbeitsabläufe, sondern ist in die Tools eingewoben, die Mitarbeitende bereits nutzen: Teams, Outlook, Slack, Gmail oder vorhandene Lernplattformen.

Sofie, der KI-Assistent, steht bereit, um Fragen zu beantworten, verdächtige E-Mails zu kennzeichnen und dringende Warnmeldungen direkt an das Personal weiterzuleiten. Policy Management und Bedrohungs-Reporting finden sich am selben Ort, sodass nichts übersehen wird. Das Ergebnis ist eine **Sicherheitskultur**, die sichtbar, messbar und auf praktische Weise im alltäglichen Betrieb präsent ist.

Artikel 21 (2) (b)	Phishing-Meldebutton
Artikel 23 (4) (a)	Sofie, KI-Copilot

Und es funktioniert. Unternehmen, die SoSafe einsetzen, berichten von einem um das **Fünffache geringeren Social-Engineering-Risiko**, einer schnelleren Meldung von Vorfällen, da mehr Mitarbeitende proaktiv handeln, und sogar niedrigeren Versicherungsprämien aufgrund der nachgewiesenen Kontrolle von Risiken durch menschliche Faktoren.

Unabhängige Prüfungen zeigen, dass **die Lösungen von SoSafe** nicht nur die Anforderungen von NIS-2 erfüllen, sondern auch von **Frameworks wie ISO 27001, DORA, TISAX, BaFin und PCI DSS**. Für Organisationen bedeutet das, dass sie die Compliance mit mehreren Standards mit einem einzigen skalierbaren System nachweisen können.

Die Plattform hat mehr als **5.500 Kunden in ganz Europa** und hilft, einen der schwierigsten Bereiche der Compliance in strukturierte, nachweisbare und nachhaltige Prozesse zu verwandeln.

So nutzen Organisationen SoSafe bereits, um die NIS-2-Anforderungen zu erfüllen:

Fellowmind hat fragmentierte Tools in fünf Ländern vereinheitlicht, um sich auf NIS-2 vorzubereiten

Fellowmind

Das Programm hat einen dedizierten Track zu **Cybersicherheit für das Management** umfasst, um Führungskräfte über ihre Haftbarkeit aufzuklären.

Erfolge:

- Phishing-Interaktionen sind um **74%** gesunken
- Simulierte Klickraten sind gefallen auf **3,5 %**
- Trainingsquoten liegen durchschnittlich bei **97%**
- Das ISO-Reporting-Toolkit hat **auditbereite Nachweise** für NIS-2, ISO und DSGVO geliefert

DEW21, ein reguliertes Energieversorgungsunternehmen, das sowohl NIS2- als auch CER-Verpflichtungen unterliegt, hat ein Programm eingeführt, das auf kontinuierlicher Praxis basiert.

DEW21

Erfolge:

- Phishing-Klickraten sind um **54%** gefallen im ersten Jahr
- Erkennung und Reporting sind auf **43%** gestiegen
- Mitarbeitende bewerteten die Trainings mit **4,9/5**
- Erstellung einer **nachverfolgbaren Nachweiskette**, um die Erwartungen der Aufsichtsbehörden zu erfüllen.

In 90 Tagen auf der Schnellspur zur Awareness-Compliance

Verwandeln Sie die NIS-2-Verpflichtungen zu menschlichen Sicherheitsrisiken mit diesem 90-Tage-Aktionsplan in praktische Maßnahmen und Nachweise, ohne Ihren Betrieb zu beeinträchtigen.

NIS-2-Cybersicherheitstraining: Implementierungscheckliste

Tage 1–30: Grundlagen und Leadership

- [ ] Führen Sie ein Briefing mit dem Management durch und planen Sie ihre Trainings.
- [ ] Segmentieren Sie die Belegschaft in Kohorten (Management, Hochrisikoteams, allgemeine Belegschaft).
- [ ] Führen Sie grundlegende Phishing- und Wissensprüfungen durch.

Tage 31–60: Gezieltes Training und Reporting

- [ ] Stellen Sie personalisierte Trainings für Mitarbeitende bereit.
- [ ] Stellen Sie rollenbasierte Module für Hochrisikoteams, nicht im Büro tätiges Personal und das Management bereit.
- [ ] Integrieren Sie den KI-Chatbot Sofie in Teams oder Slack und führen Sie ihn ein.
- [ ] Aktivieren Sie Phishing-Simulationen.
- [ ] Implementieren Sie Reporting-Tools und schulen Sie das Personal zu den entsprechenden Prozessen.
- [ ] Informieren Sie den Vorstand über den aktuellen Stand und geben Sie eine kurze Information an wichtige Zulieferer.

Tage 61–90: Vollständige Bereitstellung und Compliance

- [ ] Stellen Sie ein Nachweispaket mit Trainingsaufzeichnungen, ersten Testergebnissen und Reporting-Protokollen zusammen.
- [ ] Legen Sie klare Ziele für den Abschluss, Klickraten und Meldequoten fest.
- [ ] Führen Sie Testläufe von internen Audits durch und schließen Sie Lücken.

Machen Sie den nächsten Schritt, um sicher aufgestellt zu sein

Moderne Sicherheitsteams stehen gleich von drei Seiten auf einmal unter Druck: durch Mitarbeitende mit wenig Zeit, Angreifer, die sich ständig neu anpassen, und Auditoren, die Nachweise verlangen. NIS-2 verlangt, dass Organisationen alle drei gleichzeitig im Blick behalten, indem sie die Sicherheit zu einem elementaren Faktor in ihrer alltäglichen Arbeit machen. Ein solches Betriebsmodell wird im Laufe der Zeit von selbst immer stärker. Im Ergebnis erzielt es genau das, was am wichtigsten ist: weniger Vorfälle, nachgewiesene Compliance und eine stärkere Sicherheitskultur.

Die Expertinnen und Experten von SoSafe unterstützen Sie dabei, gemeinsam mit Ihnen dieses Modell zu gestalten, es in die Tools zu integrieren, die Ihre Mitarbeitenden bereits nutzen, und Nachweise zu erstellen, die jedem kritischen Blick standhalten. Kontaktieren Sie uns, um einen Termin zur Analyse Ihrer Bereitschaft zu vereinbaren, und verlassen Sie die Session mit einem maßgeschneiderten Plan, den Sie sofort ausführen können.

Sprechen Sie uns an