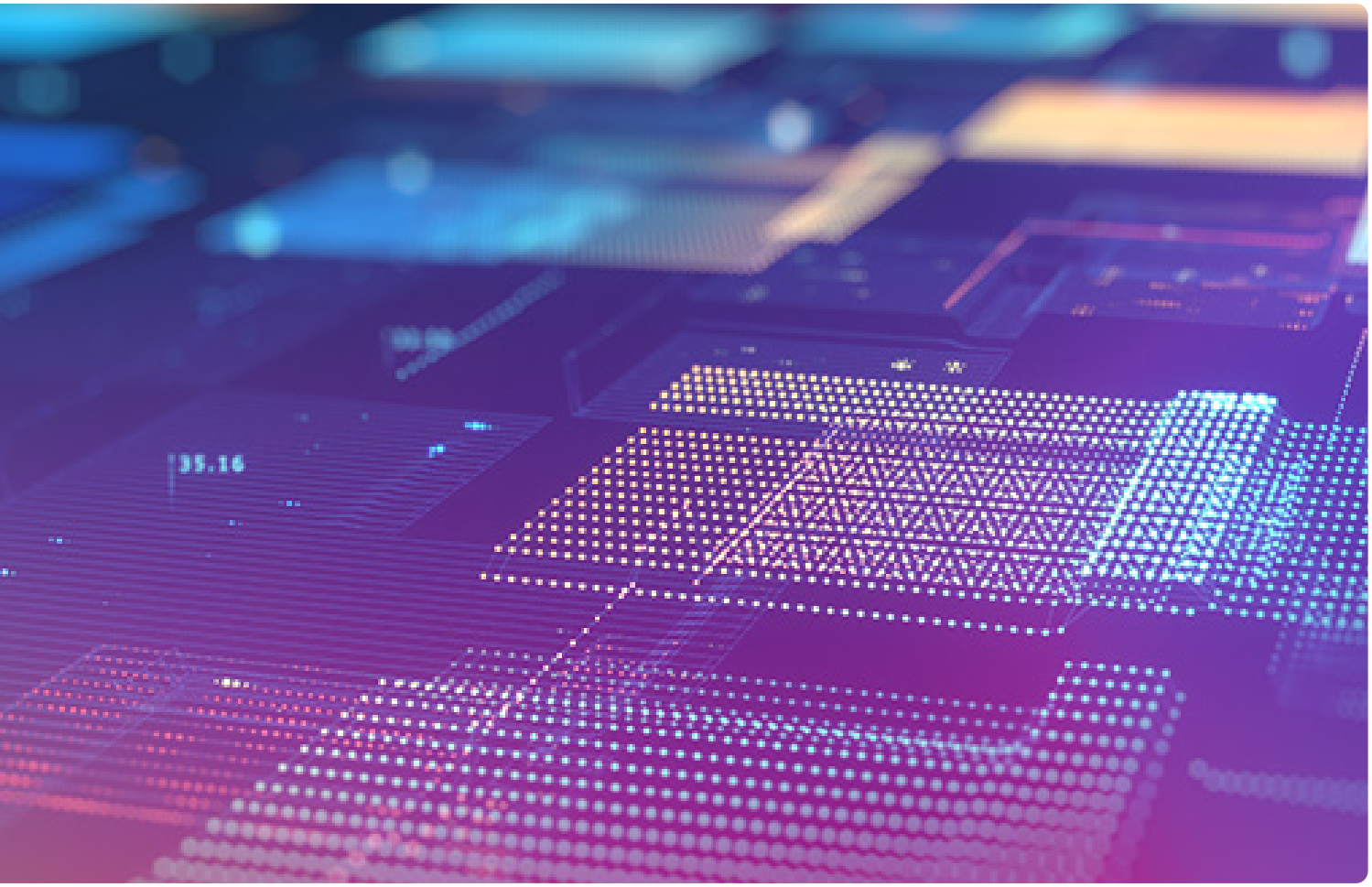
Assume Breach.

Vom Risikomanagement zur aktiven CyberResilienz unter NIS2

Für CFOs und IT-Verantwortliche



„Assume Breach“ im Kontext von NIS2

Mit dem NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) gelten seit Dezember 2025 neue, deutlich strengere Cyberverpflichtungen. Für viele Unternehmen bedeutet das nicht mehr nur die Einhaltung von Vorgaben, sondern einen grundlegenden Wandel in der Sicherheitsstrategie. Viele Unternehmen haben zunächst Self-Assessments durchgeführt; jetzt verschiebt sich der Schwerpunkt auf operative Resilienz. Genau hier setzt die „Assume Breach“-Mentalität an.

KI-gestützte und automatisierte Angriffe umgehen klassische Schutzmechanismen immer häufiger. Das Prinzip „Assume Breach“ fordert, von einer potenziellen Kompromittierung auszugehen, Erkennungs- und Reaktionsmechanismen innerhalb der IT-Infrastruktur zu verankern und Geschäftskontinuität selbst unter Druck sicherzustellen. Es geht darum, Vorfälle nicht nur zu erkennen, sondern sie schnell einzudämmen, zu beheben und systematisch daraus zu lernen.

Für Führungskräfte im Bereich Cybersecurity bedeutet „Assume Breach“ einen Paradigmenwechsel: weg von punktueller Compliance, hin zu kontinuierlicher Einsatzbereitschaft. Organisationen müssen Reaktionspläne regelmäßig testen, Teams gezielt schulen, Systeme rund um die Uhr überwachen und externe Expertise einbinden. Unternehmen sollten NIS2 und ähnliche Vorgaben nicht als Pflicht begreifen, sondern als strategische Grundlage nachhaltiger Cyberresilienz.

Eye Security befähigt Organisationen, diese Transformation erfolgreich zu gestalten und Bedrohungen nachhaltig einen Schritt voraus zu bleiben.

Marcel van Asperdt
CISO, Eye Security

Der aktuelle Stand der NIS2-Umsetzung in Deutschland

Der Bundestag hat am 13. November 2025 das NIS-2- Umsetzungsgesetz (NIS2UmsuCG) verabschiedet, womit die EURichtlinie NIS2 in deutsches Recht überführt werden soll. Das NIS2UmsuCG ist in Deutschland am 6. Dezember 2025 in Kraft getreten. Damit gelten die erweiterten Anforderungen an Cybersicherheit, Risikomanagement und Incident-Meldung nun für betroffene Organisationen. Insbesondere sind Unternehmen verpflichtet, ihre Betroffenheit zu prüfen und sich fristgerecht bei der zuständigen Aufsichtsbehörde, dem Bundesamt für Sicherheit in der Informationstechnik (BSI), zu registrieren.

Das NIS2-Umsetzungs- und Cyberresilienzstärkungs-Gesetz (NIS2UmsuCG) bringt die EU-Richtlinie NIS2 in deutsches Recht und legt den Rahmen für die Cyberresilienz „wichtiger“ und „besonders wichtiger“ Einrichtungen fest. Unternehmen müssen nachweisen, dass ihre Prozesse geeignet sind, Cyberangriffe abzuwehren. Kernpunkte sind ein erweiterter Anwendungsbereich, verpflichtendes Risikomanagement (systematische Risikoanalysen), technische und organisatorische Sicherheitsmaßnahmen, Meldepflichten bei Sicherheitsvorfällen sowie Aufsichts- und Sanktionsbefugnisse, einschließlich hoher Bußgelder.

Viele Unternehmen müssen sich darauf einstellen, dass nicht nur klassische KRITIS-Betreiber (kritische Infrastrukturen) betroffen sind, sondern auch „wichtige Einrichtungen“ außerhalb der vorherigen Definitionen. Insgesamt sollen rund 29.500 Unternehmen in Deutschland von NIS2 betroffen sein, wenn man die Kategorien „wichtige“ und „besonders wichtige“ Einrichtungen berücksichtigt.

Für Unternehmen gilt: Verzögerung ist riskant. Das Gesetz ist in Kraft, die Registrierungsfrist ist verstrichen, und EU-weite Lieferanten- und Versicherungsanforderungen verlangen bereits NIS2-konforme Nachweise.

Die Koordination der Maßnahmen übernimmt künftig das BSI in seiner Funktion als CISO Bund.

Die Aufsichtsbefugnisse der Behörde werden deutlich ausgeweitet. Stichprobenprüfungen, Nachweispflichten und Kontrollen sollen sicherstellen, dass Unternehmen die Vorgaben einhalten.

Bis zur gesetzlichen Frist am 6. März 2026 hatte sich nur ein kleiner Teil der betroffenen Unternehmen registriert — rund 11.500 von etwa 29.500. Aufgrund der niedrigen Zahlen signalisierte das BSI den Branchenverbänden, bis zum 31. Juli 2026 von Durchsetzungsmaßnahmen abzusehen. Diese informelle Kulanzfrist war keine Verlängerung der Rechtsfrist und ist inzwischen ebenfalls verstrichen. Eine fehlende Registrierung ist damit kein risikoarmes Versäumnis mehr, sondern steht im Fokus der Aufsicht. Für wesentliche Einrichtungen hat das BSI systematische Prüfungen angekündigt.

- **6. Dezember 2025** — Das NIS2UmsuCG tritt in Kraft
- **6. Januar 2026** — Das BSI-Registrierungsportal öffnet
- **6. März 2026** — Gesetzliche Registrierungsfrist (inzwischen abgelaufen)
- **31. Juli 2026** — Die informelle Kulanzfrist des BSI für verspätete Registrierungen endet
- **Aktuell** — Das BSI verlagert den Fokus auf die Compliance-Nachverfolgung ausstehender Registrierungen; für wesentliche Einrichtungen wurden systematische Prüfungen angekündigt

Das Gesetz sieht eine erweiterte Meldepflicht vor. Sicherheitsvorfälle sind innerhalb eines gestaffelten Melderegimes zu melden: die Erstmeldung innerhalb von 24 Stunden, eine Zwischenmeldung nach 72 Stunden und ein Abschlussbericht nach einem Monat.

Unabhängig von einem konkreten Vorfall ist eine Registrierung beim BSI verpflichtend; in bestimmten Fällen kann das BSI auch eine zwangsweise Registrierung anordnen.

Unternehmen sind verpflichtet, ein strukturiertes System zur Planung, Umsetzung und Überwachung der Informationssicherheit zu etablieren oder bestehende Systeme entsprechend zu erweitern, etwa durch die Einführung oder Weiterentwicklung eines Informationssicherheits-Managementsystems (ISMS). Die Maßnahmen betreffen alle zentralen Sicherheitsbereiche, von der Entwicklung von Sicherheits- und Risikokonzepten über Vorfall-, Notfall- und Krisenmanagement bis hin zu Lieferketten- und Einkaufssteuerung.

Ergänzend gehören Schulungen und Awareness-Maßnahmen, Verschlüsselung, Authentifizierung, Zugangskontrollen sowie Asset- und Schwachstellenmanagement dazu. Auch sichere Kommunikationswege und Notfallkommunikation müssen gewährleistet sein. Eine Zertifizierung nach ISO/IEC 27001:2022 oder nach BSI IT-Grundschutz kann dabei als Nachweis für die Einhaltung der Compliance-Anforderungen dienen.

Ein weiterer wesentlicher Aspekt ist die Verantwortung der Führungsebene. Geschäftsführer und Vorstände werden nicht mehr nur als Tippgeber gesehen, sondern haften aktiv für die Cyber-Resilienz ihres Unternehmens. Nach § 38 BSIG haften Geschäftsleitungen persönlich für die Umsetzung des Risikomanagements. Bei Governance-Versäumnissen drohen persönliche Bußgelder von bis zu 500.000 €, die weder auf einen CISO delegiert noch durch eine Versicherung abgedeckt werden können. Zusätzlich sind Leitungsorgane verpflichtet, mindestens alle drei Jahre an einer Cybersicherheitsschulung teilzunehmen.

Erweiterter Anwendungsbereich und Meldepflichten

Die NIS2-Cybersicherheitsvorgaben erweitern den Adressatenkreis deutlich im Vergleich zu den Vorgängervorschriften. Während diese sich vor allem auf Betreiber kritischer Infrastrukturen konzentrierten, richten sich die neuen Regeln auch an große Teile der mittelständischen Industrie. Ziel ist es, die Resilienz digitaler Prozesse zu erhöhen, unabhängig davon, ob ein Unternehmen physische Versorgungsleistungen erbringt.

Unternehmen fallen bereits dann unter NIS2, wenn ihre Tätigkeit in den im BSIG n.F. definierten Sektoren angesiedelt ist und sie als „mittleres Unternehmen“ gelten. Dies ist der Fall, sobald ein Unternehmen mehr als 50 Mitarbeiter beschäftigt oder Jahresumsatz und Bilanzsumme jeweils über 10 Mio. € liegen. Vernachlässigbare Tätigkeiten bleiben dabei unberücksichtigt.

Die erfassten Sektoren reichen von Energie, Verkehr und digitaler Infrastruktur über das verarbeitende Gewerbe bis hin zu Diensten des Digitalsektors, einschließlich Managed Services. Je größer ein Unternehmen und je relevanter sein Sektor, desto umfangreicher die Pflichten. Bestimmte Unternehmen, insbesondere in den Bereichen Digitales und Telekommunikation, sind unabhängig von ihrer Größe erfasst.

Darüber hinaus besteht eine Registrierungspflicht. Die gesetzliche Frist war der 6. März 2026 (drei Monate nach Inkrafttreten des NIS2UmsuCG) und ist damit bereits verstrichen. Das BSI hatte betroffenen Einrichtungen anschließend eine informelle Kulanzfrist eingeräumt; in seiner Kommunikation vom 31. Juli 2026 an die Branchenverbände signalisierte es, dass diese Nachsicht ausläuft und der Fokus nun auf der Nachverfolgung ausstehender Registrierungen liegt. Wer noch nicht registriert ist, sollte dies unverzüglich nachholen.

Das BSI verlangt für „besonders wichtige Einrichtungen“, „wichtige Einrichtungen“ und andere regulierte Organisationen einen zweistufigen Registrierungsprozess. Zunächst erfolgt die Anmeldung über den Dienst „Mein Unternehmenskonto“ (MUK). Anschließend müssen sich Organisationen im BSI-Portal registrieren. Nicht registrierte Einrichtungen können erhebliche Vorfälle auch über das BSI-Online-Formular melden

NIS2-Betroffenheitsprüfung starten ↗

Der Wandel von Compliance zu operativer Resilienz

Viele Unternehmen denken bei NIS2 zunächst an das Ausfüllen von Fragebögen, Audits und an den Nachweis von Maßnahmen. Doch Resilienz verlangt mehr. Es reicht nicht, Sicherheitsmaßnahmen auf dem Papier zu haben. Entscheidend ist, dass diese Maßnahmen im Alltag funktionieren.

Darum geht es nicht nur um Prävention, sondern um Erkennung, Reaktion und Wiederherstellung. Unternehmen müssen Fähigkeiten aufbauen, um Anomalien früh zu erkennen, Vorfälle professionell zu behandeln und aus ihnen zu lernen. Hierfür sind technische Mittel nötig, wie ein kontinuierliches Monitoring und Incident-Response-Pläne. Aber mindestens ebenso wichtig ist die organisatorische Vorbereitung: Verantwortlichkeiten, Eskalationspfade und Kommunikation müssen klar definiert sein.

NIS2-Umsetzung: Was können „besonders wichtige“ und „wichtige“ Einrichtungen noch heute tun? **Hier erfahren Sie mehr.**

Warum jetzt handeln wichtig ist

Seit Inkrafttreten des NIS2-Umsetzungsgesetzes sind viele der neuen Verpflichtungen unmittelbar relevant. Abzuwarten ist riskant. Unternehmen, die bereits eine strategische Umsetzung gestartet haben, verfügen über einen entscheidenden Vorteil. Sie stärken nachhaltig ihre Cyberresilienz.

Wenn Sie jetzt Ihre Sicherheitsstrategie ausrichten, schaffen Sie eine belastbare Grundlage für kontinuierliche Sicherheitsverbesserung, Risikomanagement und Nachweisführung. Darüber hinaus wird es mit Blick auf die Aufsicht durch das BSI wichtig sein, Nachweise in strukturierter Form zu erbringen. Die Dokumentation, Prozesse und technische Maßnahmen müssen auditierbar sein.

Mehr erfahren: **Bestandteile einer Risikoanalyse im Sinne der NIS2-Richtlinie**

Auch die Lieferkette spielt eine zentrale Rolle. Unternehmen müssen sich nicht nur um ihre eigenen Risiken kümmern, sondern auch die Cyber-Resilienz ihrer Dienstleister, Partner und Zulieferer stärker in den Blick nehmen. In der Praxis heißt das, dass Verträge, Prozessketten und Zugriffsrechte neu bewertet werden müssen, um künftigen NIS2-Verpflichtungen gerecht zu werden.

Mehr erfahren: **Best-Practice-Empfehlungen für Anforderungen an Lieferanten**

Ist Ihr IT-Team dafür gerüstet?

Viele Organisationen gehen davon aus, dass ihre internen IT-Teams sämtliche Aspekte der Cybersecurity abdecken können. In der Praxis werden moderne Bedrohungen jedoch zunehmend komplexer und stammen häufig aus legitimen Konten vertrauenswürdiger Beteiligter, was ihre Erkennung und Abwehr erschwert. Selbst besonders aufmerksame Mitarbeitende können Opfer solcher Angriffe werden. Da Angreifer heute auf professionellem Niveau agieren, ist eine ebenso qualifizierte Gegenstrategie erforderlich: Fachleute mit entsprechender Ausbildung und Erfahrung, die hochentwickelte Bedrohungen erkennen, einordnen und neutralisieren können.

Die meisten internen IT-Teams verfügen nicht dauerhaft über die Ressourcen, um auf diesem Niveau zu operieren. Auch Managed Service Provider (MSPs) leisten wertvolle Unterstützung, verfügen jedoch möglicherweise nicht über die Tiefe an Fachwissen oder Kapazitäten eines spezialisierten Cybersecurity- Anbieters.

Für Organisationen, die NIS2-Anforderungen zuverlässig erfüllen möchten, kann die Zusammenarbeit mit einem Managed Detection & Response (MDR)-Anbieter oder die Implementierung eines strukturierten Cybersecurity- Frameworks entscheidend sein.

Dies gewährleistet, dass Vorfälle von erfahrenen Fachleuten bearbeitet, Bedrohungen rund um die Uhr überwacht und Cybersecurity-Praktiken validiert sowie zertifiziert werden.

Was bei Nicht-Einhaltung droht

Wenn ein Unternehmen seine Pflichten unter dem NIS2UmsuCG nicht erfüllt, können erhebliche Konsequenzen folgen. Das BSI könnte verpflichtende Sicherheitsmaßnahmen anordnen oder bei schweren Mängeln sogar eine externe Aufsicht einsetzen. Darüber hinaus drohen empfindliche Bußgelder.

Das Bußgeldsystem orientiert sich am weltweiten Konzernumsatz und unterscheidet zwischen „besonders wichtigen“ und „wichtigen“ Einrichtungen. Besonders wichtige Einrichtungen können mit bis zu 10 Mio. € oder bis zu 2 % des weltweiten Jahresumsatzes belegt werden, während bei wichtigen Einrichtungen Bußgelder von bis zu 7 Mio. € oder bis zu 1,4 % des weltweiten Jahresumsatzes drohen.

Neben finanziellen Sanktionen sind auch weitergehende Aufsichtsmaßnahmen, behördliche Anordnungen und die persönliche Verantwortlichkeit der Leitung möglich. Unternehmen riskieren zudem nicht nur finanzielle Schäden, sondern auch Reputationsverlust, wenn sie als unsichere Partner wahrgenommen werden.

Wie bei der DSGVO zählen verspätete oder unvollständige Meldungen sowie unzureichende Sicherheitsmaßnahmen zu den häufigsten Auslösern für Sanktionen. Unternehmen sollten daher sicherstellen, dass Meldepflichten eingehalten, Sicherheitsmaßnahmen angemessen umgesetzt und Verantwortlichkeiten klar definiert sind, um finanzielle und regulatorische Risiken zu minimieren.

Das Gesetz signalisiert damit unmissverständlich, dass Cyberresilienz und Compliance künftig Kernaufgaben der Unternehmensführung sind.

Ihr Fahrplan zur NIS2-Compliance

NIS2-Umsetzungsroadmap: Von der Analyse zur nachhaltigen Resilienz.

Ein zentraler Baustein ist ein kontinuierliches Überwachungs- und Erkennungsmodell. Dieser Ansatz verstärkt Ihre Fähigkeit, Angriffe nicht nur zu verhindern, sondern frühzeitig zu erkennen und mit professionellen Maßnahmen zu reagieren. Ergänzend dazu ist ein modernes Incident-ResponseProgramm essenziell. Dieses Programm muss realistische Szenarien abdecken, Meldewege definieren und Verantwortlichkeiten klar regeln, damit im Ernstfall schnell reagiert werden kann.

Die Anforderungen von NIS2 verlangen, dass Sie nicht nur Ihre eigenen Systeme, sondern auch Ihre Partner auf ihr Cyber-Risikoprofil hin prüfen. Dafür müssen Verträge angepasst, Audits durchgeführt und Sicherheitsstandards mit Dritten vereinbart werden.

Auf Managementebene empfehlen sich gezielte Schulungen, damit Führungskräfte ihre Rolle in der Cyber-Strategie verstehen. Nur wenn alle Stakeholder ein gemeinsames Verständnis für Risiken, Strategie und Verantwortlichkeiten haben, wird eine nachhaltige Resilienz möglich.

1 Betroffenheitsprüfung

Prüfen Sie, ob Ihr Unternehmen unter Berücksichtigung branchenspezifischer Kriterien in den Anwendungsbereich des BSIG n. F. fällt. Ist dies der Fall, bereiten Sie die Registrierung bei der gemeinsamen Registrierungsstelle von BSI vor und benennen Sie eine interne Kontaktstelle.

2 Assessment. Standortbestimmung und Gap-Analyse

Zu Beginn erfolgt eine umfassende Analyse der bestehenden Sicherheits-, Compliance- und Governance-Strukturen. Dazu gehören die Prüfung relevanter Dokumentationen (Policies, Prozesse, Nachweise) sowie strukturierte Interviews mit Schlüsselrollen aus IT, Security, Recht, Einkauf, Risiko und Management. Ziel ist eine realistische Einschätzung des aktuellen Reifegrads, der NIS2-relevanten Lücken und der organisatorischen Verantwortlichkeiten.

3 Roadmap. Maßnahmenplanung und Priorisierung

Auf Grundlage des Assessments wird eine praxisnahe, risikoorientierte Roadmap entwickelt. Diese enthält fachliche, organisatorische und technische Maßnahmen, priorisiert nach Wirksamkeit, Aufwand, Abhängigkeiten und geschäftskritischen Risiken. Budgets, Rollen, Zeitpläne sowie notwendige Skills oder Partnerressourcen werden festgelegt.

4 Design und Implementierung. Aufbau und Integration von Sicherheitsarchitekturen

In dieser Phase werden Zielprozesse (z. B. Incident Handling, Reporting, Monitoring), Rollenmodelle (inkl. Management-Aufsichtspflichten) sowie technische und organisatorische Kontrollen nach NIS2 definiert und stufenweise implementiert. Dazu zählen u. a. den Aufbau oder Anpassung eines Informationssicherheits-Managementsystems (ISMS) nach den BSIG-neu-Vorgaben; dokumentierte Policies, Verantwortlichkeiten und Prozesse (Security Controls, Notfall- und Krisenmanagement, Lieferkettenprozesse, Awareness-Programme und Reporting-Strukturen).

5 Betrieb, Monitoring und kontinuierliche Verbesserung

Nach der Implementierung werden die Systeme, Prozesse und Kontrollen in den Regelbetrieb überführt und kontinuierlich überwacht. Dazu gehören KPI-gestütztes Reporting, regelmäßige Reviews, Audits, Übungen (z. B. Tabletop- oder Red-Team-Simulationen) sowie die fortlaufende Optimierung gemäß aktueller Bedrohungslage, regulatorischer Änderungen und Lessons Learned. Kritische Assets identifizieren, Bedrohungen bewerten, Sicherheitsmaßnahmen priorisieren; regelmäßige Risiko-Reviews implementieren.

6 Meldepflichten und Nachweisführung für Compliance vorbereiten

Beginnen Sie frühzeitig damit, Dokumentationen, Logs, Berichte und weitere Nachweise zu sammeln, die die Einhaltung der Sorgfaltspflichten („Due Care“) belegen. Ziehen Sie zudem eine ISO-27001-Zertifizierung in Betracht, falls noch nicht vorhanden. Sie bietet eine solide Grundlage und genießt breite Anerkennung. Dazu sollten Sie Prozesse für zeitnahe Erfassung, Klassifikation und Meldung von Sicherheitsvorfällen etablieren und Schnittstellen zu Behörden definieren.

7 Lieferketten und Verträge prüfen

Anforderungen von Kunden, Partnern und Versicherungen auf NIS2-Konformität prüfen und vertraglich absichern: Prüfen Sie die Cybersicherheitsmaßnahmen Ihrer zentralen Dienstleister und Lieferanten durch regelmäßige Audits. Legen Sie zudem vertragliche Sicherheitsanforderungen fest, die sich an den künftigen NIS2-Pflichten orientieren.

8 Kontinuierliche Compliance. Langfristige Resilienz verankern („Assume Breach“)

Etablieren Sie kontinuierliche Detection-, Threat-Hunting- und Response-Fähigkeiten. Richten Sie Ihre Sicherheitsstrategie konsequent auf Cyberresilienz aus.

Unternehmen, die jetzt proaktiv handeln, reduzieren nicht nur rechtliches Risiko, sondern stärken die operative Resilienz und verschaffen sich strategische Vorteile gegenüber Wettbewerbern. Die NIS2-konforme Vorbereitung sollte integraler Bestandteil der Cyberstrategie sein, nicht nur eine regulatorische Pflicht.

Unterstützung durch Eye Security

Um die Cyberresilienz Ihrer Organisation zu erhöhen und auf potenzielle Bedrohungen vorbereitet zu sein, bietet Eye Security gezielte Services, die eine solide Grundlage für Risikominimierung und Schutz vor Cyberangriffen schaffen.

Ein zentraler Service ist Managed Extended Detection and Response (MXDR). Er vereint die kontinuierliche Überwachung von Endpunkten sowie von On-premises- und Cloud-Identitäten mit einer strukturierten Nachbereitung von Sicherheitsvorfällen. Ziel ist es, Angriffe frühzeitig zu erkennen, ihre Auswirkungen zu begrenzen und eine schnelle, fachkundige Reaktion sicherzustellen. Expertinnen und Experten begleiten den gesamten Prozess, von der ersten Analyse bis zur vollständigen Wiederherstellung.

Im Ernstfall unterstützen Incident-Response-Expertinnen und -Experten bei allen notwendigen Schritten, von der technischen Wiederherstellung betroffener Systeme bis hin zur fristgerechten Meldung an die zuständigen Behörden.

Darüber hinaus bietet Eye Security Awareness-Programme für Mitarbeitende an. Durch Schulungen, regelmäßige PhishingSimulationen und praxisnahe Trainings werden Mitarbeitende darin geschult, potenzielle Cyberbedrohungen frühzeitig zu erkennen und angemessen zu reagieren, was die Sicherheitslage der gesamten Organisation stärkt.

Die kombinierte Nutzung technischer Schutzmaßnahmen und organisatorischer Sensibilisierung trägt dazu bei, Sicherheitsrisiken systematisch zu reduzieren und die Compliance-Anforderungen zu unterstützen.

Jetzt Kontakt aufnehmen. Erfahren Sie, wie Eye Security Ihr Unternehmen gezielt schützen und die Cyberresilienz nachhaltig stärken kann.

© 2026 Eye Security. Alle Rechte vorbehalten. Die in dieser Veröffentlichung enthaltenen Informationen dienen ausschließlich allgemeinen Informationszwecken und stellen keine vertraglichen oder sonstigen Verpflichtungen dar. Obwohl die Inhalte sorgfältig geprüft wurden, übernimmt Eye Security keine Gewähr für die Richtigkeit, Vollständigkeit oder Aktualität der Inhalte. Jegliche Haftung, insbesondere für direkte oder indirekte Schäden, die aus der Nutzung oder Nichtnutzung der Informationen entstehen, ist im gesetzlich zulässigen Umfang ausgeschlossen. Alle Leistungsbeschreibungen unterliegen den geltenden Vertragsbedingungen, Ausschlüssen und Konditionen. Diese Veröffentlichung ersetzt keine individuelle Beratung oder vertragliche Vereinbarungen.