eye.

Visit eye.security

Der vollständige Leitfaden für die Umsetzung von NIS2 in Deutschland

Vorwort von Job Kuijpers

Cyberangriffe haben verheerende wirtschaftliche Folgen – und noch weitere tiefgreifende Auswirkungen. Sie bedrohen die demokratischen Grundprinzipien der gesamten Europäischen Union und unsere freie und offene Gesellschaft. Im schlimmsten Fall stört ein Cyberangriff sogar die Funktionsfähigkeit unseres Landes.

Als Reaktion auf die jüngste und rasche Eskalation der Internetkriminalität hat die Europäische Union beschlossen, die NIS-Richtlinie zu erneuern. Ziel der Änderungen an NIS2 ist es, die Widerstandsfähigkeit der europäischen Organisationen und damit der EU insgesamt zu verbessern.

Die neue Richtlinie betrifft nicht nur alle Organisationen, die bisher unter NIS fielen, sondern darüber hinaus auch weitere Betriebe mit gesellschaftlicher Verantwortung.

Es gibt viele Gründe, schon heute auf eine verbesserte Cybersicherheit hinzuarbeiten. Wer sich nicht an die NIS2 hält, dem drohen bald Geldstrafen und andere Sanktionen. . Aber Cybersicherheit ist weitaus mehr als die Einhaltung von Vorschriften und die Minimierung eines Angriffsrisikos.

Eine solide Cyberabwehr schützt nicht nur Ihr Unternehmen, Ihre Mitarbeiter und Ihre Systeme, sondern auch Ihre Kunden und andere Stakeholder – und letztlich die Gesellschaft als Ganzes. Im Falle einer Störung tragen der verantwortungsvolle Umgang und die Meldung dazu bei, das Bewusstsein anderer zu schärfen und zu verhindern, dass sich ähnliche Fehler wiederholen.

Jeder möchte sich auf gut funktionierende Dienste und ein Umfeld verlassen können, in dem sensible und personenbezogene Daten sicher bleiben. Dabei kann jede Organisation einen Teil dazu beitragen, eine sichere und vertrauenswürdige Gesellschaft zu ermöglichen.

Unabhängig davon, wie klein Ihre Organisation ist, sind Sie ein Glied in einer größeren Kette. Nur wenn alle mitmachen, können wir die gesamte Kette und die Gesellschaft so sicher wie möglich halten. Eye Security ist bereit, Sie genau dabei zu unterstützen.

TIMELINE NIS2 - FÜR DAS BILD IM BEISPIEL

28. November 2022:
Annahme der NIS2-Richtlinie durch den Europäischen Rat

Januar 2023:
Die Umsetzungsfrist von 21 Monaten beginnt. Innerhalb dieser Frist muss die Richtlinie in nationales Recht umgesetzt werden

21. Juni 2024:
Der Referentenentwurf des Bundesministeriums des Innern und für Heimat wurde in überarbeiteter Fassung veröffentlicht, muss aber noch verabschiedet und verkündet werden.

17. Oktober 2024:
Stichtag für die Umsetzung der NIS2-Richtlinie in den EU-Mitgliedstaaten. Sowohl in Deutschland als auch in anderen Staaten wird es zu Verspätungen kommen.

Q1-Q2 2025:
Voraussichtlich in diesem Zeitraum können Unternehmen mit dem Inkrafttreten von NIS 2 rechnen

NIS2: Was, warum und wann?

Die Richtlinie zur Netz- und Informationssicherheit (NIS) ist eine europäische Richtlinie zur Verbesserung der Cybersicherheit und der Widerstandsfähigkeit wichtiger und besonders wichtiger Einrichtungen in den EU-Mitgliedstaaten.

In den letzten Jahren sind die Cyber-Bedrohungen sprunghaft angestiegen, und die Wahrscheinlichkeit von Störungen nimmt zu. Deshalb hat die Europäische Union an einem Nachfolger der NIS gearbeitet: der NIS2, die Ende 2022 verabschiedet wurde.

Beide Richtlinien zielen darauf ab, die Cybersicherheit in für die Gesellschaft wichtigen Organisationen zu verbessern. Eingestuft als wichtige oder besonders wichtige Einrichtungen, werden mit NIS2 eine Reihe von Sicherheitsanforderungen verbindlich. Mit NIS2 werden mehr Sektoren und Organisationen abgedeckt. Besonderes Augenmerk liegt auf der kritischen Infrastruktur (KRITIS). Für alle erfassten Organisationen wird es verschärfte Anforderungen im Bereich der Cybersicherheit geben.

Die NIS2-Richtlinie wurde zwar bereits auf europäischer Ebene verabschiedet, muss aber erst in nationales Recht überführt werden. Erst dann ist das Einhalten der Vorschrift verpflichtend. In Deutschland handelt es sich um das “Gesetz der Umsetzung von EU NIS2 und Stärkung der Cybersicherheit”, kurz NIS2UmsuCG. NIS2 wird in Deutschland etwa 30 Tsd. Unternehmen betreffen.

Wenn die NIS2-Richtlinie für Ihr Unternehmen gilt, müssen Sie sich offiziell registrieren – mit Informationen zu beispielsweise Ihrer Einrichtung, der Rechtsform, Kontaktdaten, der Tätigkeit der Einrichtung, Sektor und Branche. Details des Registrierungsverfahrens sind noch nicht bekannt, werden aber auf der Webseite des Bundesamts für Sicherheit in der Informationstechnik (BSI) veröffentlicht.

Wenn Sie auf dem Laufenden gehalten werden möchten, können **Sie sich hier** für eine E-Mail-Benachrichtigung von Eye Security anmelden.

Wer ist von NIS2 betroffen?

Es gibt zwei Arten von Organisationen, die von NIS2 betroffen sind: wichtige Einrichtungen und besonders wichtige Einrichtungen. Ob Sie die NIS2 einhalten müssen – und in welche der beiden Kategorien Sie fallen – hängt von der Branche ab, in der Ihre Organisation tätig ist, von der Größe Ihres Unternehmens sowie von Ihrem Umsatz und der Bilanzsumme.

Die folgenden Organisationen fallen unter die NIS2-Richtlinie:

- Große Organisationen: Organisationen mit mindestens 250 Beschäftigten UND/ODER mit einem Jahresumsatz von mehr als 50 Millionen Euro und einer Bilanzsumme von mehr als 43 Millionen Euro. Diese Organisationen fallen immer unter die NIS2 und werden als besonders wichtig angesehen, sofern sie in einem der in Sektor 1 aufgeführten Wirtschaftszweige tätig sind. Wenn die Geschäftstätigkeit in Sektor 2 aufgeführt ist, wird die Organisation als wichtig eingestuft.
- Mittlere Unternehmen: Unternehmen mit mehr als 50 Beschäftigten UND/ODER mit einem Jahresumsatz von mehr als 10 Millionen Euro und einer Bilanzsumme von mehr als 10 Millionen Euro. Diese Organisationen können unter die NIS2 fallen, wenn sie in einem der als wichtig oder besonders wichtig eingestuften Sektoren tätig sind. Die nachstehende Abbildung zeigt, welche Sektoren zu diesen Sektoren gehören.
- Kleine Organisationen: Einrichtungen mit weniger als 50 Beschäftigten können von NIS2 betroffen sein, wenn sie zu den kritischen Infrastrukturen (KRITIS) gehören.
- Zulieferer von wichtigen oder besonders wichtigen Organisationen sind NICHT direkt von der NIS2 betroffen. Indirekt jedoch schon, da die NIS-regulierten Organisationen in der EU verpflichtet sind, ihren Lieferanten Anforderungen aufzuerlegen.

Die offizielle Dokumentation der Richtlinie enthält eine detaillierte Beschreibung, welche Art von Organisationen und Geschäftstätigkeiten unter die einzelnen betroffenen Sektoren fallen. Ein Unternehmen fällt unter die NIS2 Richtlinie, wenn zwei Bedingungen erfüllt sind: Unternehmensgröße und Sektor. Die 18 NIS2 Sektoren ähneln den KRITIS Sektoren, die vom BSI festgelegt worden sind. KRITIS Organisationen haben Bedeutung für das staatliche Gemeinwesen. Fallen sie aus oder ist der Geschäftsablauf gestört, kommt es zu Versorgungsengpässen oder Störung der öffentlichen Sicherheit.

Unternehmen und Einrichtungen müssen selbständig herausfinden, ob sie von NIS2 betroffen sind und wie sie die Richtlinie umsetzen.

↘ Möchten Sie wissen, ob Ihr Unternehmen von NIS2 betroffen ist? **Machen Sie unseren Test**, der auf den neuesten verfügbaren Informationen basiert.

Wie wird die Umsetzung von NIS2 in Organisationen aussehen?

Derzeit sind die genauen Regulationen der NIS2 auf nationaler Ebene noch nicht verabschiedet. Es ist also noch nicht genau definiert, was Organisationen umsetzen müssen, um der NIS2-Richtlinie zu entsprechen. Wesentliche Aspekte stehen aber bereits fest. Denn das übergeordnete Ziel sollte nicht nur sein NIS2 einzuhalten, sondern die Risiken von Cyberattacken zu minimieren.

Sicher ist, dass Organisationen im Rahmen der NIS2 einer **Sorgfaltspflicht** und einer Meldepflicht nachkommen müssen.

Die Sorgfaltspflicht umreißt die wichtigen Cybersicherheitspraktiken, die jedes Unternehmen umsetzen muss. Dazu gehören Risikomanagement, Informationssicherheit entlang der Lieferkette, Business Continuity Management, das Einrichten von Verschlüsselungen und mehrstufiger Authentifizierung, Schulungen und Weiterbildungen zum Thema Cybersecurity und das Einrichten von Kontaktstellen, sowie die Einführung der Meldepflicht.

Die Meldepflicht beinhaltet verschiedene Regularien für den Umgang mit Sicherheitsvorfällen. Tritt ein schwerer Sicherheitsvorfall ein, muss er innerhalb der kurzen Frist von 24 Stunden an das BSI gemeldet werden. Nach 72 Stunden ist eine Bestätigung erforderlich und ein Abschlussbericht innerhalb des Monats nach dem Vorfall. Mit Rückfragen seitens des BSI ist zu rechnen.

Die Einhaltung der NIS2 wird von verschiedenen Aufsichtsbehörden überwacht. Organisationen mit hoher Kritikalität werden proaktiv überwacht, hier ist mir Vor-Ort-Besuchen und stichprobenartigen Kontrollen zu rechen. Im Sektor mit sonstiger Kritikalität wird nur reaktiv kontrolliert, etwa beim Verdacht auf Verstöße.

Was ist, wenn ich NIS2 nicht einhalte?

Die NIS2 enthält eine Reihe von Sanktionen für Organisationen, die den Vorschriften nicht entsprechen. So kann eine Aufsichtsbehörde von einer Organisation verlangen, den betreffenden Mangel offenzulegen und Maßnahmen zu ergreifen, um innerhalb eines bestimmten Zeitrahmens die Vorschriften einzuhalten. Letztendlich führt ein Verstoß von NIS2 aber schnell zu empfindlichen Geldbußen.

Für KRITIS Organisationen und besonders wichtige Einrichtungen beträgt die Geldbuße maximal 10 Millionen Euro oder 2 % des gesamten weltweiten Jahresumsatzes im vorangegangenen Geschäftsjahr. Wichtige Organisationen müssen bei Verstößen mit Geldbußen von bis zu 7 Mio. EUR oder 1,4 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres rechnen.

Darüber hinaus können Geschäftsführer und weitere Führungsgremien mit ihrem Privatvermögen haftbar gemacht werden.

Diese hohen Geldbußen dienen neben der Abschreckung noch einem weiteren Zweck: Unternehmen müssen die Gelegenheit nutzen, um ihre Cybersecurity-Maßnahmen auf den Prüfstand zu stellen. Effiziente Maßnahmen minimieren nicht nur unnütze Ausgaben, sondern minimieren auch das Risiko von Cyberattacken.

Gute Cybersicherheit zahlt sich aus – das Gesamtpaket von Eye Security beispielsweise hat einen ROI von 300 %.

↘ **Weitere Informationen über die Meldepflicht und die Sorgfaltspflicht finden Sie auf der Website von Eye Security.**

NIS2 – Wo soll ich anfangen?

Vieles an NIS2 ist noch unklar, unter anderem auch wann genau die Vorschrift in Kraft treten wird. Unabhängig davon sollten Sie jetzt Maßnahmen ergreifen! Bis Ihre Organisation den Anforderungen vollständig entsprechen wird, kann es eine Zeit dauern. Aber auf dem Weg dahin können Sie aktiv daran arbeiten, das Risiko von Cyberangriffen zu minimieren. So schützen Sie sich vor wirtschaftlichen und reputations bezogenen Schäden.

Mit diesen drei Schritten können Sie beginnen:

1

Prüfen Sie, ob Sie unter die NIS2 fallen

Sie können bereits jetzt prüfen, ob Sie unter die NIS2 fallen und, falls ja, ob Ihre Organisation als wichtig oder besonders wichtig einzustufen ist. Eye Security hat einen **Compliance-Check** entwickelt, der Ihnen zeigt, ob Sie die NIS2 einhalten müssen.

2

Registrieren Sie sich so bald wie möglich

Als Organisation obliegt es Ihnen selbst, sich zu identifizieren und beim BSI zu registrieren. Dabei gelten unterschiedliche Registrierungsregeln: Besonders wichtige und wichtige Einrichtungen müssen sich innerhalb von drei Monaten beim BSI registrieren. KRITIS-Betreiber müssen zusätzliche Informationen bereitstellen. Die 3-Monatsfrist für die Registrierung läuft am 17. Januar 2025 ab, bis dahin müssen sich alle Organisationen beim BSI registriert haben.

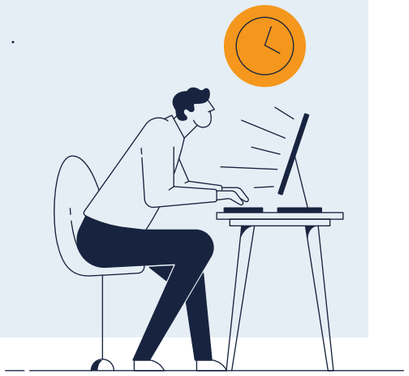
Wenn Sie informiert werden möchten, sobald die Registrierung möglich ist, können **Sie sich hier** für eine E-Mail-Benachrichtigung von Eye Security anmelden.

3

Prüfen Sie, wie konform Sie bereits sind

Im Vorfeld von NIS2 können Sie bereits Maßnahmen ergreifen, um die Cyber-Resilienz Ihres Unternehmens zu verbessern. Möchten Sie wissen, wie konform und widerstandsfähig Sie bereits sind? Mit dem **kostenlosen NIST-Scan von Eye Security** finden sie es heraus.

.



So kann Eye Security Sie unterstützen

Möchten Sie aktiv mit der Erfüllung der NIS2-Anforderungen beginnen und Ihre Cyber-Resilienz erhöhen? Eye Security kann Ihnen helfen.

Eine der obligatorischen Sicherheitsmaßnahmen im Rahmen von NIS2 ist der Umgang mit Störfällen. Mit dem Managed Extended Detection and Response Service kann Eye Security Sie hier unterstützen. Wir helfen Ihnen nicht nur bei der Reaktion auf Vorfälle, sondern überwachen auch Ihre Endpunkte und die Cloud, um Cyberangriffe zu verhindern.

Darüber hinaus erfordert NIS2 grundlegende Cybersicherheitsmaßnahmen und Schulungen. Eye Security bietet einen optionalen Awareness-Service an, der regelmäßige Phishing-Simulationen und zusätzliche Schulungen für Mitarbeiter umfasst, die auf solche E-Mails hereinfallen.

Möchten Sie das Risiko von Cyberattacken senken und potenzielle Schäden vermeiden? Dann schauen Sie sich unser umfassendes Cyber-Schutzpaket an oder kontaktieren Sie uns. Wir helfen Ihnen gerne weiter.

↘ Möchten Sie mehr über die NIS2 erfahren?
Besuchen Sie unser NIS2 **Informationszentrum**.

eye.