LEITFADEN

NIS2-Leitfaden für Unternehmen: Diese Maßnahmen sind jetzt wichtig, wenn Sie betroffen sind.

proliance

Status quo bei der IT-Sicherheit: Unternehmen im Visier von Cyberkriminellen

Wie ist die Lage der IT-Sicherheit in Deutschland – diese Frage stellt das Bundesamt für Sicherheit in der Informationstechnik (BSI) jedes Jahr. Für 2023 lautet die Antwort: Die Lage ist „angespannt bis kritisch“.

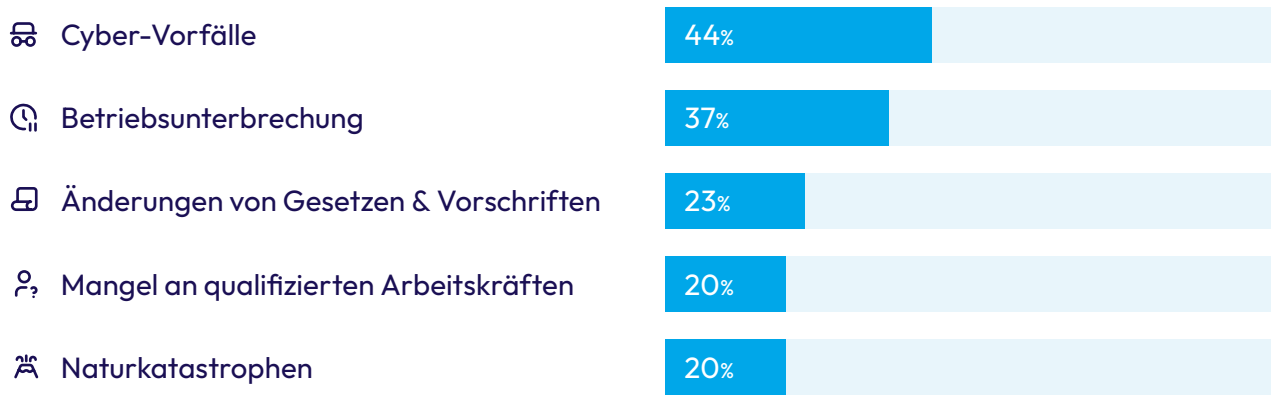
Vor allem Ransomware stellt eine zunehmende Bedrohung dar. Darunter versteht man Schadprogramme, die Cyberkriminelle nutzen, um Unternehmen zu erpressen. Hacker können damit zum Beispiel Daten von Unternehmen verschlüsseln und geben diese nur gegen Lösegeld wieder frei. Zudem entstehen durch technologische Entwicklungen wie Künstliche Intelligenz neue Schwachstellen und bieten eine zusätzliche Angriffsfläche für Hacker.

Zusammen mit Datenschutzverletzungen und IT-Unterbrechungen stellen Cybervorfälle wie Ransomware-Attacken die **größte Sorge für Unternehmen weltweit** dar. In Deutschland gibt die Mehrheit der Organisationen sogar an, die eigene **Existenz durch Cyberangriffe bedroht** zu sehen.

> **Die Bedrohung im Cyberraum ist so hoch wie nie zuvor.**

Quelle: „Die Lage der IT-Sicherheit in Deutschland 2023“, Bundesamt für Sicherheit in der Informationstechnik

Top 5 Geschäftsrisiken in Deutschland in 2024



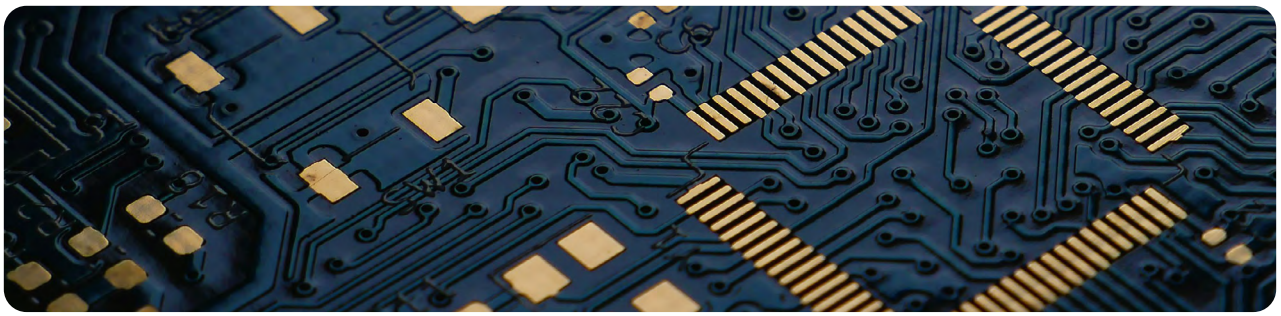
Quelle: „Allianz Risk Barometer: Cyber-Attacken als weltweites Top-Risiko 2024“, Allianz

Das BSI mahnt deshalb, dass Organisationen mehr Resilienz erreichen und ihre IT-Sicherheit priorisieren sollten. Sonst drohen sie, zur Zielscheibe für immer gefährlichere Cyberangriffe zu werden. Die NIS2-Richtlinie ist einer der Schlüssel dafür.

52 %

der Unternehmen sehen ihre Existenz durch Cyberangriffe bedroht.

Quelle: Studie „Wirtschaftsschutz 2023 “, Bitcom



Fakten zu NIS2 im Kurzüberblick

- Die NIS2 ist die Überarbeitung einer bestehenden Richtlinie über Netz- und Informationssicherheit (NIS).
- Die EU hatte die ursprüngliche Richtlinie 2016 eingeführt, um auf die zunehmende Bedrohung durch Cyberangriffe zu reagieren. 2022 wurde eine Neuauflage beschlossen, da die Bedrohungslage sich immer weiter verschärft.
- Zu den Neuerungen gehören umfangreichere Schutzmaßnahmen, die Unternehmen treffen müssen, strengere Meldepflichten bei Sicherheitsvorfällen, strengere Aufsicht durch die Behörden und mehr Pflichten für die Geschäftsführung. Bei Nichterfüllung der NIS2-Direktive drohen Sanktionen.
- Für Unternehmen in Deutschland gilt das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG). Es verpflichtet etwa 30.000 Unternehmen in Deutschland erstmals gesetzlich dazu, hohe Informationssicherheitsstandards einzuhalten.
- Ziel der neuen Richtlinie ist es, Unternehmen und Behörden resilienter zu machen, um sie und die Bevölkerung zu schützen. Außerdem fördert NIS2 die Kooperation von Staat und Wirtschaft.
- Unternehmen sollten frühzeitig damit beginnen, ihre Sicherheitsstandards zu erhöhen. Im Vorteil sind Organisationen, die bereits über ein Information Security Management System (ISMS) nach ISO 27001 verfügen.

NIS2: Was bedeutet die Richtlinie für Ihr Unternehmen?

Die NIS2 ist die Antwort der Europäischen Union auf die wachsende Cyberkriminalität – und soll genau die Resilienz fördern, zu der das BSI dringend rät.

Betroffen sind nicht nur die klassischen Betreiber kritischer Infrastrukturen wie Energie- und Wasserversorger, Telekommunikationsanbieter oder Transportunternehmen.

NIS2 erweitert den Kreis deutlich und nimmt auch zahlreiche andere Unternehmen in die Pflicht. So müssen künftig auch Firmen, die Teil komplexer Lieferketten sind, ihre Abwehrmaßnahmen gegen Angriffe aus dem Netz verbessern.

30.000

Unternehmen und Organisationen könnten Expertenschätzungen zufolge von NIS2 betroffen sein.

Zudem hat die EU die Pflichten, die sich aus der Direktive ergeben, im Vergleich zu NIS1 deutlich verschärft – ebenso wie die Sanktionen, die bei Missachtung drohen. Möglich sind Bußgelder, Betriebsunterbrechungen und persönliche Haftungsrisiken.

Unternehmen müssen jetzt handeln

Um Strafen zu vermeiden und ihre IT-Infrastruktur zu schützen, müssen Unternehmen jetzt prüfen,

- ✓ ob sie von der NIS2-Richtlinie betroffen sind,
- ✓ welche Maßnahmen in Vorbereitung auf das Inkrafttreten von NIS2 zu treffen und zu verstärken sind, und
- ✓ wie sie ihre IT-Sicherheit aufrechterhalten und langfristig stärken können.

Ist Ihr Unternehmen betroffen? Dann müssen Sie sich mit dem Inkrafttreten von NIS2 bei der zuständigen nationalen Behörde registrieren. Danach müssen Sie Vorfälle melden und die Einhaltung der Sicherheitsanforderungen gewährleisten.

⚠ **Vorsicht:** Ob Ihr Unternehmen unter die NIS2-Richtlinie fällt und Sie meldepflichtig sind, müssen Sie selbst ermitteln und sich proaktiv bei der zuständigen Behörde registrieren. In Deutschland ist die Meldung an das BSI zu richten.

Vorteile von NIS2 für Unternehmen

Auf Organisationen und Behörden in Deutschland, die unter die NIS2 fallen, kommt viel Arbeit zu. Doch die Übertragung der Richtlinie auf die eigenen Prozesse lohnt sich, wie folgende Vorteile zeigen:

Mehr Sicherheit: Die NIS2-Richtlinie hat das Ziel, Ihre Cybersecurity zu stärken, damit Ihr Unternehmen besser vor finanziellen Schäden und Datenverlusten geschützt ist, die regelmäßig durch Cyberattacken entstehen.

Besseres Risikomanagement: Die NIS2 verpflichtet Sie dazu, Ihre IT-Systeme regelmäßig auf mögliche Risiken und Schwachstellen zu prüfen. Sie müssen also zwangsläufig Ihr Risikomanagement verbessern – damit reduzieren Sie gleichzeitig die Wahrscheinlichkeit eines Angriffs auf Ihre IT-Systeme.

Unterstützung für Ihren Datenschutz: IT-Sicherheit stärkt nicht nur die Cyber-resilienz, sondern auch Ihren Datenschutz. Denn je besser Ihre Systeme geschützt sind, desto schwerer haben Hacker es, auf Ihre Daten zuzugreifen.

Höheres Kundenvertrauen: Mehr Datensicherheit bedeutet auch, dass Ihre Kunden-daten besser abgesichert sind. Dadurch steigt das Vertrauen Ihrer Kunden in Ihr Handeln.

Reibungsloser Geschäftsbetrieb: Um die NIS2-Anforderungen zu erfüllen, benötigen Sie in Zukunft einen Plan zur Aufrechterhaltung des Betriebs im Falle eines Angriffs. Dazu gehören zum Beispiel Backup-Pläne, die Unternehmen auch unabhängig von der Bedrohungslage im Cyberspace haben sollten.

Wer muss sich auf NIS2 vorbereiten?

Grundsätzlich betrifft die Richtlinie die Betreiber kritischer Infrastrukturen, die in einer von 18 definierten Sektoren tätig sind. 11 Sektoren, darunter die Bereiche Energie und digitale Infrastruktur, sind als hoch kritisch eingestuft. Weitere 7 Sektoren, wie die Abfallbranche oder die produzierende Industrie, gelten als kritisch. Außerdem gilt die „ size-cap rule“.

Was ist die „size-cap rule“?

Diese Regel bedeutet: Nur mittlere und große Vertreter der 18 Sektoren fallen unter die Richtlinie.

- **Mittlere Unternehmen** haben mindestens 50 Angestellte oder einen jährlichen Mindestumsatz von 10 Millionen Euro.
- **Große Unternehmen** haben mindestens 250 Beschäftigte oder einen jährlichen Mindestumsatz von 50 Millionen Euro.

Kleinere Unternehmen mit weniger als 50 Mitarbeitern oder unter 10 Millionen Euro Jahresumsatz fallen nicht unter die NIS2-Richtlinie. Ausnahme: Die Tätigkeit des Unternehmens hat kritische Auswirkungen auf die öffentliche Ordnung oder ein Betriebsausfall würde Systemrisiken verursachen.

Sind Sie von der NIS2-Richtlinie betroffen?

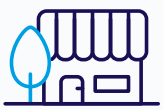
Hochkritische Sektoren:

- Energie
- Verkehr
- Bankwesen
- Finanzmarktinfrastruktur
- Gesundheit
- Trinkwasser
- Abwasser
- Digitale Infrastruktur
- Verwaltung von IKT-Diensten (B2B)
- öffentliche Verwaltung
- Weltraum

Kritische Sektoren:

- Post- und Kurierdienste
- Abfallbewirtschaftung
- Produktion, Herstellung und Handel mit chemischen Stoffen
- Produktion, Verarbeitung und Vertrieb von Lebensmitteln
- Verarbeitendes Gewerbe/Herstellung von Waren
- Anbieter digitaler Dienste
- Forschung

JA



Kleines Unternehmen
max. 50 Beschäftigte
oder max. 10 Mio. €
Umsatz

Mittleres Unternehmen
mind. 50 Beschäftigte
oder 10 Mio. €
Umsatz

Großes Unternehmen
mind. 250 Beschäftigte
oder über 50 Mio. €
Umsatz

NIS2 trifft nicht zu

NIS2 trifft zu

Ist Ihr Unternehmen bereit für NIS2?
Ermitteln Sie Ihren NIS2-Compliance-Status in nur 10 Minuten. Einfach. Schnell. Aussagekräftig.

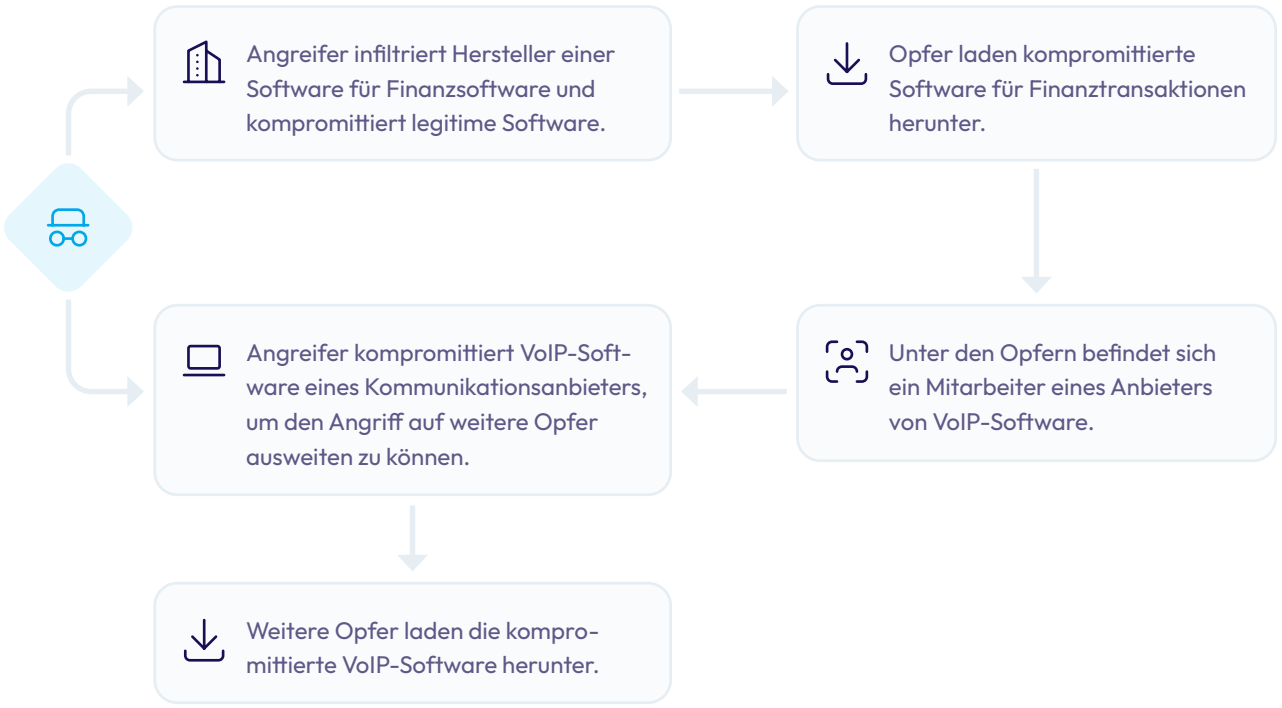
Zum interaktiven Selbsttest

Achtung: NIS2 betrifft auch Lieferketten

Die Richtlinie schreibt vor, dass auch Ihre Zulieferer oder Dienstleister Sicherheitsmaßnahmen ergreifen müssen, um Ihre Prozesse nicht zu gefährden. Denn Hacker können Schwachstellen in Lieferketten problemlos nutzen, um zum Beispiel kompromittierte Software über verbundene Partner zu verteilen und damit großen Schaden anzurichten.

In bestehenden und künftigen Verträgen mit Partnern und Zulieferern wird deshalb zu prüfen sein, ob alle Vertragsparteien ihre Prozesse und IT-Systeme ausreichend schützen.

Supply-Chain-Angriff infolge eines Supply-Chain-Angriffs



Quelle: „Die Lage der IT-Sicherheit in Deutschland 2023“, Bundesamt für Sicherheit in der Informationstechnik

So schützen Autobauer ihre Lieferketten

Die Automobilindustrie setzt für erweiterte IT-Sicherheit über die eigenen Unternehmensgrenzen hinaus die TISAX-Zertifizierung ein. Mit diesem Prüfmechanismus gewährleisten Hersteller, dass Zulieferer und Partner höchste Sicherheitsstandards einhalten und keine sensiblen Daten an die Öffentlichkeit gelangen.

Mehr zu TISAX®erfahren

*TISAX® ist eine eingetragene Marke der ENX Association. Die Proliance GmbH steht in keiner geschäftlichen Beziehung mit der ENX Association Mit der Nennung der Marke TISAX® ist keine Aussage des Markeninhabers zur Geeignetheit der hier beworbenen Leistungen verbunden.

Ihr Unternehmen fällt unter die NIS2? Diese Pflichten kommen auf Sie zu

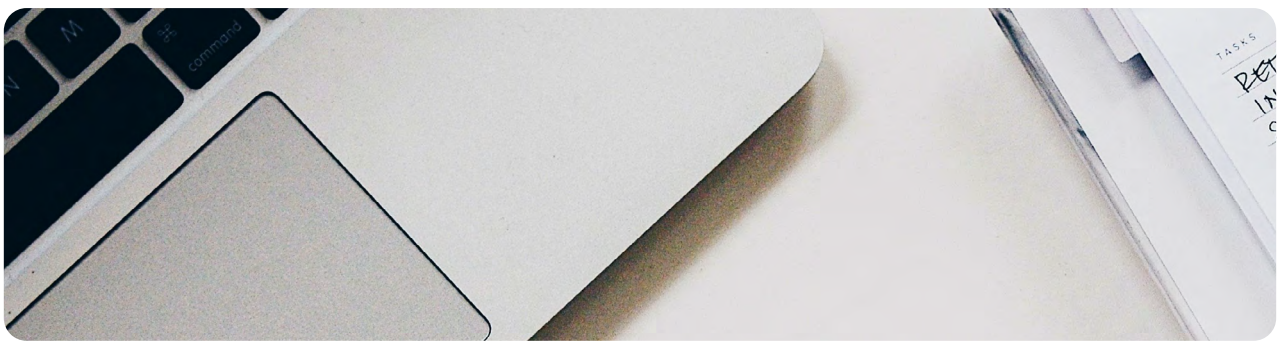
Die NIS2-Richtlinie sieht eine Reihe von Pflichten für Unternehmen vor, aber auch für die Führungsebene. Das sind die wichtigsten Fakten im Überblick.

1 Maßnahmen zum Risikomanagement

Die Richtlinie verlangt von betroffenen Einrichtungen und Unternehmen, mindestens die folgenden Cybersecurity-Maßnahmen umzusetzen:

- Konzepte für die Risikoanalyse und IT-Sicherheit
- Verhüten, Erkennen, Analysieren und Eindämmen von Sicherheitsvorfällen
- Aufrechterhaltung des Betriebs (Business Continuity)
- Sicherheit in der Lieferkette
- Sicherheit beim Erwerben, Entwickeln und Warten der IT-Systeme
- Bewertung der Wirksamkeit von Risikomanagementmaßnahmen
- Schulungen im Bereich der Cybersicherheit und „Cyberhygiene“ (sichere Passwörter, Backups usw.)
- Kryptografie und Verschlüsselung für sichere Authentifizierung
- Sicherheit des Personals und Konzepte für die Zugriffskontrolle
- Sichere Kommunikationswege im Daily Business und im Notfall

Für diese Maßnahmen sieht die Richtlinie einen gefahrenübergreifenden Ansatz vor – das bedeutet: Sie müssen Ihre IT-Systeme mitsamt ihrer physischen Umgebung schützen.



2 Meldepflichten bei Sicherheitsvorfällen

Erhebliche Sicherheitsvorfälle müssen dem BSI umgehend gemeldet werden. Diese Fristen gelten dabei:

spätestens innerhalb von 24 Std. nach Kenntnisnahme
Frühwarnung, ggf. mit Verdacht, dass der Vorfall rechtswidrig oder böswillig erfolgt ist und ob grenzüberschreitende Auswirkungen drohen

spätestens innerhalb von 72 Std. nach Kenntnisnahme
Aktualisierte Meldung mit erster Bewertung der Schwere und Auswirkung des Vorfalls und ggf. Angaben zu Kompromittierungsindikatoren

spätestens innerhalb eines Monats nach Übermittlung der aktualisierten Meldung
Abschlussbericht mit ausführlicher Beschreibung des Vorfalls inklusive Schweregrad und Auswirkungen (ggf. grenzüberschreitend), Angaben zu der Art der Bedrohung, der möglichen Ursache und der getroffenen Abhilfemaßnahmen

3 Registrierung

Wenn NIS2 für Sie relevant ist, müssen Sie sich innerhalb von drei Monaten nach Inkrafttreten der NIS2 selbstständig beim BSI registrieren.

4 Sicherheit in der Lieferkette

Direkt betroffene Unternehmen müssen sicherstellen, dass in ihrer Lieferkette keine Sicherheitsrisiken für die eigene IT-Security bestehen.

5 Pflichten für die Geschäftsführung

Zu den wichtigen Änderungen der NIS2 gehören neue Pflichten für die Geschäftsführung. Cybersecurity wird mit NIS2 Chefsache. Leitende Angestellte, die das Thema nicht ernst nehmen, haften persönlich.

Die neue Richtlinie sieht vor, dass Geschäftsführer Cybersecurity-Maßnahmen ergreifen und ihre Umsetzung im Unternehmen überwachen müssen. Sie sind darüber hinaus verpflichtet, Schulungen wahrzunehmen und anzubieten, um die Belegschaft zu sensibilisieren.

Welche Sanktionen drohen bei Verstößen?

Unternehmen, die unter NIS2 fallen, ist die Einhaltung der Vorgaben dringend geraten. Sonst drohen empfindliche Strafen. Auf Unternehmen, die nicht NIS2-konform sind, kommen folgende Geldbußen zu (es gilt jeweils der höhere der beiden Beträge):

- **Wichtige Einrichtungen:** Bis zu 7 Mio. € oder 1,4 % des weltweiten Vorjahresumsatzes
- **Wesentliche Einrichtungen:** Bis zu 10 Mio. € oder 2 % des gesamten weltweiten Vorjahresumsatzes
- **Besonders schwere Fälle:** Bis zu 20 Mio. € oder 4 % des Vorjahresumsatzes weltweit

Darüber hinaus sind die Behörden unter Umständen befugt, ein Aussetzen Ihres Geschäftsbetriebs anzuordnen. Hinzu kommen die persönlichen Haftungsrisiken für Führungskräfte.

Ausgewählte Schadenssummen 2023

	Schaden in Mrd.
Imageschaden	35,3
Ausfall, Diebstahl oder Schädigung von Informations- u. Produktions-systemen oder Betriebsabläufen	35,0
Kosten für Rechtsstreitigkeiten	29,8
Kosten für Ermittlungen und Ersatzmaßnahmen	25,2
Umsatzeinbuße durch Verlust von Wettbewerbsvorteilen	21,5
Erpressung mit gestohlenen oder verschlüsselten Daten	16,1
. . .	
Gesamtsumme	**205,9**

Quelle: Studie „Wirtschaftsschutz 2023 “, Bitcom

über

200 Mrd. €

kosteten Cyberattacken im Jahr 2023 den deutschen Unternehmen

Cyberresilienz lohnt sich

Führen Sie sich vor Augen, dass ein Cyberschaden ohne Sicherheitsmaß-nahmen in der Regel weitaus größer ist als unter Einhaltung der NIS2. Denn ein Sicherheitsvorfall zieht nicht nur Imageschäden, sondern Kosten für Rechtsverfahren, Umsatzverluste, Lösegelder und Datenschutzverstöße nach sich.

Was muss ich jetzt tun?

Um Sanktionen zu vermeiden und Ihre IT zu schützen, sind folgende Schritte notwendig:

Finden Sie zunächst heraus, ob Ihre Organisation von der NIS2-Direktive betroffen ist – nutzen Sie dafür die Expertise von Proliance und finden Sie in einem kostenfreien Beratungsgespräch mit uns gemeinsam heraus, ob NIS2 für Sie relevant ist. Prüfen Sie anschließend die NIS2-Anforderungen im Detail und registrieren Sie sich rechtzeitig beim BSI.

Nach einer Risikobewertung und einer Bestandsaufnahme der bereits bestehenden Maßnahmen für IT-Sicherheit sollten Sie Schwachstellen identifizieren und festlegen, wie Sie die Lücken schließen können – das gilt auch für Ihre Lieferketten.

Als nächstes setzen Sie die Anforderungen der NIS2 um, legen Pläne für den Umgang mit Sicherheitsvorfällen fest und bieten Schulungen für Ihre Mitarbeiter an. Die umgesetzten Maßnahmen müssen von nun an überwacht und optimiert werden.

Rund um die neue NIS2-Richtlinie gibt es viel zu tun – je früher Sie starten, desto besser. Proliance unterstützt Sie dabei und stellt sicher, dass Sie Ihre Pflichten rund um die Cyber-security erfüllen, Ihre IT-Systeme und Daten schützen und trotzdem weiter produktiv sein können.

Tipp: NIS2 mit ISO 27001-Zertifizierung einfacher umsetzen

Wenn Ihre Organisation der NIS2-Richtlinie unterliegt, hilft ein zertifiziertes ISMS Ihnen, die Vorgaben der Richtlinie einfacher zu erfüllen. Risikobewertung, Pläne für den Ernstfall und die Umsetzung von technischen Sicherheitsmaßnahmen sind Voraussetzungen für eine Zertifizierung von ISMS nach ISO 27001 – und gehören gleichzeitig zu den von NIS2 geforderten Maßnahmen. Durch eine Zertifizierung zeigen Sie Ihren Kunden und Partnern außerdem, dass Cybersicherheit zu Ihren Prioritäten gehört und Sie den Schutz Ihrer IT-Systeme und Daten ernstnehmen.

Ihre zukunftsfähige ISMS-Lösung: Proliance InfoSec

Wir beraten Sie gern dazu, wie Sie eine Zertifizierung für Ihr ISMS erhalten und behalten und die NIS2-Anforderungen sicher einhalten. Lernen Sie unsere ISMS-Lösung Proliance Infosec kennen – für mehr IT-Security und weniger Cyberrisiken.

Jetzt unverbindlich beraten lassen

Sie haben Fragen?
Wir helfen Ihnen weiter!

Sie wünschen eine unverbindliche Beratung
zu Compliance in Ihrem Unternehmen?

Rufen Sie uns gerne an oder schreiben Sie uns
eine E-Mail!

proliance.ai
+49 (0)89 250 039 220
info@proliance.ai

Alexander Ingelheim
Geschäftsführung

Compliance. Sicher erledigt.
Proliance ist die Datenschutz- und Compliance-Plattform für den Mittelstand. Wir kombinieren smarte Software mit persönlicher Beratung durch TÜV- und Dekra-zertifizierte Experten und Compliance-Enthusiasten, damit Sie DSGVO, NIS2, ISO 27001, TISAX® u.a. mühelos erfüllen. Risikofrei, unkompliziert, zeitsparend. Über 2.500 Kunden aus 50+ Branchen vertrauen seit 2017 auf uns.

proliance

Join the movement
Wir sind Mitglied

We take
Climate
Action
lfca.earth/co2