IT BUSINESS **LÖSUNGEN**

SpaceNet

NIS2 verstehen und umsetzen:

Ein praxisnaher Leitfaden für mittelständische Unternehmen

PERSÖNLICH.
STARK.
SICHER.
KLUG.
RICHTIG GUT.

Inhalt

Executive Summary

Die NIS2-Richtlinie der EU markiert einen Wendepunkt für die Cybersicherheit in Europa – insbesondere für mittelständische Unternehmen. Erstmals werden tausende mittelständische Betriebe in verschiedenen Sektoren direkt in die Pflicht genommen, ein hohes Maß an IT-Sicherheit nachzuweisen[1][2]. Geschäftsführungen und Vorstände tragen nun eine persönliche Verantwortung für die Cybersicherheit und können bei Versäumnissen haftbar gemacht werden.

Dieses Whitepaper bietet einen umfassenden Überblick darüber, was NIS2 verlangt, wen es betrifft und wie betroffene Unternehmen die Vorgaben praxisnah umsetzen können. Schritt für Schritt zeigen wir, wie Sie ein angemessenes Sicherheitsniveau etablieren – von der Risikoanalyse über technische und organisatorische Maßnahmen bis hin zu Incident-Response-Prozessen und kontinuierlichem Monitoring. Wir beleuchten typische Herausforderungen im Mittelstand (z. B. begrenzte Ressourcen und Know-how) und wie diese überwunden werden können. Zudem erfahren Sie, welche Rolle ein externer Managed Security Service Provider (MSSP) wie SpaceNet bei der NIS2-Compliance spielen kann, untermauert durch ein konkretes Praxisbeispiel. Am Ende wissen Sie, worauf es ankommt, um NIS2 konform zu werden, und wie Sie mit erfahrenen Partnern Ihr Unternehmen effektiv schützen und alle rechtlichen Vorgaben erfüllen können.

Cybersicherheit wird mit NIS2 zur Führungsaufgabe. Erstmals verpflichtet die Richtlinie Geschäftsführungen und Vorstände ausdrücklich dazu, Cyberrisiken aktiv zu steuern, Sicherheitsmaßnahmen zu billigen und deren Umsetzung regelmäßig zu überwachen. Versäumnisse können nicht nur zu hohen Bußgeldern führen, sondern auch zu persönlicher Haftung der Leitungsorgane. Damit ist NIS2 kein reines IT-Thema mehr, sondern Teil der unternehmerischen Sorgfaltspflicht und der Corporate Governance. Unternehmen sind gefordert, Cybersicherheit strategisch zu verankern und nachvollziehbar zu dokumentieren.

Einleitung

Die digitale Bedrohungslage entwickelt sich rasant – und mittelständische Unternehmen geraten zunehmend ins Visier von Cyberkriminellen. Während Großunternehmen oft über dedizierte Security-Teams und ausgefeilte Abwehrmechanismen verfügen, sind kleine und mittlere Unternehmen (KMU) häufig schlechter geschützt. Studien zeigen die Dringlichkeit: 81 % der Unternehmen in Deutschland waren bereits Opfer eines Cyberangriffs, was 2024 zu einem geschätzten Gesamtschaden von über 266 Milliarden Euro führte. Besonders alarmierend ist, dass Angriffe auf den Mittelstand stark zunehmen und für viele betroffene Firmen existenzbedrohend sein können. Gründe dafür liegen unter anderem darin, dass IT-Sicherheit in vielen mittelständischen Betrieben bislang nicht als strategische Priorität verankert war. Gleichzeitig setzen Angreifer auf immer raffiniertere Methoden – von gezielten Phishing-Kampagnen über Ransomware bis hin zu DDoS-Angriffen –, die speziell auf die Schwachstellen von KMUs abzielen.
Vor diesem Hintergrund hat die Europäische Union mit der zweiten Network and Information Security Richtlinie (NIS2) reagiert. Die 2024 in Kraft getretene Richtlinie zielt darauf ab, das Cybersicherheitsniveau EU-weit anzuheben und Unternehmen zu proaktiven Sicherheitsmaßnahmen zu verpflichten. Nach einigem Hängen und Würgen bei der nationalen Umsetzung in Deutschland, auch bedingt durch den Regierungswechsel im Mai 2025, wurde das NIS2-Umsetzungsgesetz (NIS2UmsuCG) am 13. November 2025 vom Bundestag beschlossen, vom Bundesrat gebilligt und ist am 6. Dezember 2025 in Kraft getreten.

Während die ursprüngliche NIS-Richtlinie von 2016 nur kritische Infrastrukturen (KRITIS) wie Energie- oder Wasserversorger betraf, weitet NIS2 den Geltungsbereich nun deutlich aus. Insbesondere mittelständische Unter-nehmen in wichtigen Wirtschaftssektoren fallen neu unter die Regulierung. Damit wird Cybersicherheit für viele Betriebe vom optionalen Good-Practice zum gesetzlich bindenden Muss.

Die NIS2-Richtlinie verpflichtet Unternehmen, ein angemessenes und dokumentiertes Sicherheitsniveau zu gewährleisten. Das bedeutet: Sie müssen Risiken fortlaufend managen, technische und organisatorische Schutzmaßnahmen einführen, Mitarbeitende schulen und Sicherheitsvorfälle unverzüglich melden. Verstöße gegen diese Pflichten sind keine Lappalie – es drohen empfindliche Bußgelder bis 10 Millionen € oder 2 % des weltweiten Jahresumsatzes sowie die eingangs erwähnte persönliche Haftung der Geschäftsleitung. Gerade dieser Aspekt – die Haftung von Führungskräften – stellt eine erhebliche Verschärfung dar und unterstreicht, dass Cybersecurity Chefsache ist.

Für mittelständische Geschäftsführungen, IT-Leitungen und CISOs bedeutet dies: Sie müssen sich jetzt intensiv mit NIS2 auseinandersetzen. Dieses Whitepaper unterstützt Sie dabei, die Relevanz der NIS2-Richtlinie zu verstehen und in praxisnahe Handlungsschritte zu übersetzen. Zunächst klären wir die Hintergründe von NIS2 und wen die neuen Regeln betreffen. Anschließend beleuchten wir detailliert, welche Anforderungen erfüllt werden müssen und welche Herausforderungen speziell im Mittelstand auftreten. Ein 8-Punkte-Plan zeigt Ihnen Schritt für Schritt, wie Sie die Umsetzung angehen können.

In Kapitel 8 erfahren Sie, wie die SpaceNet AG Sie als kompetenter Sicherheitspartner begleiten kann – von Managed Security Services bis hin zu Schulungen – illustriert durch ein Beispiel aus der Praxis. Abschließend fassen wir die wichtigsten Punkte zusammen und geben Empfehlungen für die nächsten Schritte auf dem Weg zur NIS2-Compliance, inklusive einem Hinweis auf einen unverbindlichen NIS2-Check.

NIS2 im Überblick –
Hintergrund und Entwicklung

Dieser Zeitstrahl zeigt die wichtigsten Meilensteine von NIS2 – von der EU-Gesetzgebung bis zur Umsetzung in deutsches Recht.

Die Network and Information Security Directive 2, kurz NIS2, ist die überarbeitete Fassung der ersten NIS-Richtlinie von 2016. Sie wurde von der EU beschlossen, um auf die dramatisch gewachsene Cyber-Bedrohungslage zu reagieren und EU-weit ein höheres Sicherheitsniveau zu etablieren. NIS2 trat auf EU-Ebene im Jahr 2024 in Kraft und musste von den Mitgliedstaaten binnen 21 Monaten in nationales Recht überführt werden. Für Deutschland bedeutete dies eine Frist bis Oktober 2024. In der Praxis wurde das nationale NIS2-Umsetzungsgesetz allerdings erst im Laufe des Jahres 2025 finalisiert und ist seit dem 5. Dezember 2025 in Kraft.

Was ist das Ziel von NIS2?

Kurz gesagt: Die digitale Resilienz von Unternehmen und staatlichen Stellen soll verbessert werden. Die EU möchte Fragmentierung vermeiden und einen einheitlichen Mindeststandard für Cybersicherheit etablieren. Jedes Mitgliedsland richtet dafür eine zuständige Behörde ein (in Deutschland das BSI, Bundesamt für Sicherheit in der Informationstechnik), welche die Einhaltung überwacht. Durch NIS2 sollen Vorfälle wie großflächige IT-Ausfälle, Datenlecks oder Sabotageakte besser verhindert, oder falls sie doch eintreten, schneller gemeldet und bewältigt werden.

Was hat sich gegenüber der alten NIS-Richtlinie geändert?

Einige der wichtigsten Neuerungen sind:

> Erweiterter Geltungsbereich: NIS2 erfasst deutlich mehr Unternehmen (siehe nächster Abschnitt), insbesondere auch solche mittlerer Größe. Die Kategorisierung in wesentliche und wichtige Unternehmen wurde eingeführt, um die Kritikalität abzubilden.

> Strengere Pflichten: Die Anforderungen an das Risikomanagement, die technischen Maßnahmen und die Berichtswege wurden konkretisiert und verschärft (Details in Abschnitt 4). Beispielsweise sind nun definierte Meldezeiten für Sicherheitsvorfälle vorgegeben.

> Höhere Sanktionen: Bußgelder und Konsequenzen (bis hin zur persönlichen Haftung) wurden angehoben, um die Verbindlichkeit zu erhöhen.

> Verantwortung der Führungsebene: NIS2 nimmt explizit das Top-Management in die Pflicht. Die Geschäftsleitung muss sich aktiv um Cybersecurity kümmern und haftet für Versäumnisse – dies war in der alten Richtlinie so nicht vorgesehen.

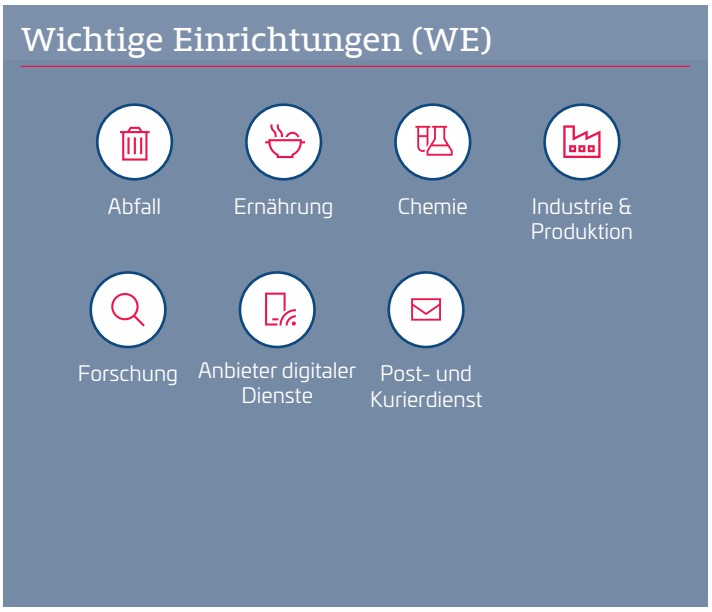
> Stärkere Zusammenarbeit: Die EU-Mitgliedstaaten und deren Sicherheitsbehörden sollen enger kooperieren und Informationen über Cyberbedrohungen austauschen. Dies hilft insbesondere bei grenzüberschreitenden Vorfällen.

Für mittelständische Unternehmen bedeutet diese Richtlinie einen Paradigmenwechsel. Viele Betriebe, die bislang wenig Berührung mit regulativen Anforderungen in der IT-Sicherheit hatten, müssen sich nun binnen kurzer Zeit auf neue Compliance-Vorgaben einstellen. Im nächsten Abschnitt schauen wir uns an, welche Unternehmen konkret betroffen sind und wie man herausfindet, ob das eigene Unternehmen dazu gehört.

Wer ist von NIS2 betroffen?

Unter NIS2 fallen wesentlich mehr Unternehmen als zuvor unter NIS1. Die Richtlinie unterscheidet zwei Kategorien von betroffenen Organisationen[19]:

Besonders wichtige Einrichtungen (BWE) – dies entspricht im Wesentlichen den ehemaligen kritischen Infrastrukturen, also Organisationen, deren Ausfall erhebliche Auswirkungen auf Gesellschaft und Staat hätte.



Wichtige Einrichtungen (WE) – dies ist eine neue Kategorie, die Unternehmen umfasst, die zwar nicht zur kritischen Infrastruktur zählen, aber dennoch in wichtigen Wirtschaftszweigen tätig sind und bestimmte Schwellenwerte überschreiten.

Welche Branchen sind adressiert?

Das Spektrum wurde bewusst breit gefasst. Betroffen sind Unternehmen aus den Bereichen Energie, Transport & Verkehr, Gesundheit, Trinkwasser und Abwasser, digitale Infrastruktur, Chemie, Abfallwirtschaft, Lebensmittelversorgung sowie Teile des verarbeitenden Gewerbes. Zur digitalen Infrastruktur zählen z. B. Cloud-Dienste, Rechenzentren, Hosting- und DNS-Anbieter, die nun unabhängig von ihrer Größe als kritisch eingestuft sein können. Auch Finanzdienstleister und Versicherungen gehören dazu, wobei für den Finanzsektor zusätzlich die separate EU-Verordnung DORA gilt (Digital Operational Resilience Act, siehe Hinweis unten).

Beispiele für typische mittelständische Unternehmen, die neu unter NIS2 fallen können, sind: ein Maschinenbauunternehmen mit europaweiten Lieferketten, ein Pharma-Mittelständler, ein regionales Logistikunternehmen, ein Software- oder IoT-Dienstleister mit kritischen Kunden, oder auch ein Betreiber eines Colocation-Rechenzentrums. Wichtig ist, dass nicht allein die Branche entscheidet, sondern auch die Betriebsgröße:

Schwellenwerte

In der Regel greift NIS2 für private Unternehmen, wenn sie mindestens 50 Mitarbeiter beschäftigen oder mehr als 10 Mio. € Jahresumsatz bzw. Bilanzsumme haben. Das heißt, klassische KMU im Sinne der EU-Definition (kleiner als 50 MA und <10 Mio. Umsatz) sind ausgenommen – es sei denn sie gehören zu bestimmten besonders sensiblen Sektoren. Einige Bereiche – wie etwa Trust-Dienste (z. B. DNS-Server) oder bestimmte Cloud- und Hosting-Anbieter – sind unabhängig von der Unternehmensgröße als kritisch definiert und fallen somit unter NIS2, auch wenn sie klein sind.

Öffentliche Einrichtungen:

Nicht nur Unternehmen, auch staatliche Stellen können betroffen sein, sofern sie in den relevanten Sektoren agieren (z. B. kommunale Wasserwerke, Krankenhäuser in öffentlicher Trägerschaft, etc.). Die genaue Abgrenzung ist im nationalen Umsetzungsgesetz geregelt. In Deutschland definiert das NIS2-Umsetzungsgesetz (auch "Cybersecurity-Stärkungsgesetz" genannt) die betroffenen Einrichtungen und lässt das BSI Schwellenwerte regelmäßig überprüfen und anpassen.

Für Unternehmen, die nicht sicher sind, ob sie unter NIS2 fallen, empfiehlt sich ein Abgleich mit den Kriterien oder eine Anfrage beim BSI. Oft gibt es branchenspezifische Leitfäden (z. B. von Kammern oder Verbänden) und Online-Tools, um die eigene Betroffenheit einzuschätzen. Klar ist jedoch: Weite Teile des gehobenen Mittelstands – insbesondere in industriellen und digitalen Branchen – zählen nun zu den „wichtigen Einrichtungen" und haben damit neue Pflichten.

Hinweis:

Für den Finanz- und Bankensektor gilt ergänzend die Verordnung DORA, die parallel zu NIS2 Cyber-Resilienz verlangt. DORA und NIS2 sind teils überschneidend – Finanzunternehmen müssen beide Rahmenwerke beachten. Dieses Whitepaper fokussiert auf NIS2; Finanzunternehmen sollten jedoch DORA nicht außer Acht lassen.

Bin ich von NIS2 betroffen?

Ein Unternehmen fällt unter die NIS2-Richtlinie, wenn mindestens eines der folgenden Kriterien erfüllt ist:

> Tätigkeit in einem der definierten Sektoren, z. B. verarbeitendes Gewerbe, Energie, Gesundheit, Transport & Logistik, digitale Infrastruktur oder Anbieter digitaler Dienste

> Mindestens 50 Mitarbeitende oder mehr als 10 Mio. € Jahresumsatz bzw. Bilanzsumme

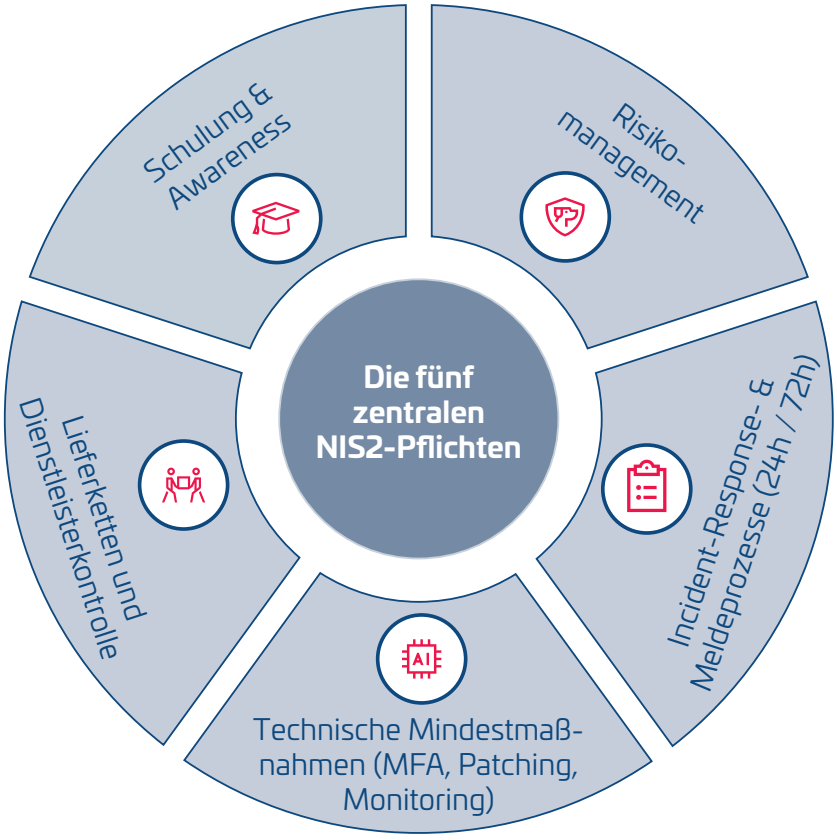
> Unabhängig von der Unternehmensgröße, wenn das Unternehmen als systemrelevant gilt, etwa als Cloud-, Hosting-, DNS- oder Rechenzentrumsanbieter

Für viele Unternehmen des gehobenen Mittelstands bedeutet dies, dass sie erstmals unter eine verbindliche Cybersicherheitsregulierung fallen. Eine frühzeitige Prüfung der eigenen Betroffenheit ist daher essenziell.

Was fordert die NIS2-Richtlinie?

Im Zentrum der NIS2-Richtlinie steht das risikobasierte Cyberrisikomanagement.
Alle weiteren Anforderungen – von technischen Sicherheitsmaßnahmen über Schulungen bis hin zu Meldepflichten – leiten sich aus einer strukturierten Risikoanalyse ab. Unternehmen müssen Cyberrisiken systematisch identifizieren, bewerten und geeignete Gegenmaßnahmen festlegen. Entscheidend ist dabei nicht ein maximaler Sicherheitsgrad, sondern ein angemessenes, nachvollziehbares und dokumentiertes Sicherheitsniveau auf Basis des Standes der Technik.

Die NIS2-Richtlinie legt einen umfangreichen Katalog an Sicherheitsanforderungen fest, den betroffene Unternehmen erfüllen müssen. Wichtig ist, dass es nicht nur um technische Lösungen geht, sondern um ein ganzheitliches Sicherheitsmanagement, das im ganzen Unternehmen verankert ist. Im Kern lassen sich die Pflichten in folgende Bereiche gliedern:



Die fünf zentralen NIS2-Pflichten für Unternehmen

Aus Sicht des Mittelstands lassen sich die Anforderungen der NIS2-Richtlinie auf fünf zentrale Pflichtbereiche verdichten:

> Etabliertes Risikomanagement zur kontinuierlichen Bewertung von Cyberrisiken
> Definierte Incident-Response- und Meldeprozesse, inklusive Einhaltung der 24-/72-Stunden-Fristen
> Technische Mindestmaßnahmen wie MFA, Patch-Management, Protokollierung und Monitoring
> Kontrolle von Lieferketten und IT-Dienstleistern hinsichtlich Cybersicherheit
> Regelmäßige Schulungen für Mitarbeitende und Führungskräfte
> Unternehmen müssen diese Maßnahmen nicht nur umsetzen, sondern auch jederzeit gegenüber Aufsichtsbehörden nachweisen können.

a) Risikomanagement etablieren:

Unternehmen müssen ein formales Risikomanagement für IT- und Informationssicherheit betreiben. Konkret heißt das: Sie haben regelmäßig eine Risikoanalyse durchzuführen, die Bedrohungen und Schwachstellen systematisch identifiziert. Anschließend sind die Risiken zu bewerten (wie wahrscheinlich ist ein Szenario, wie gravierend wären die Auswirkungen?) und entsprechende Gegenmaßnahmen abzuleiten. Dieser Prozess muss dokumentiert und kontinuierlich wiederholt werden. Ein Ergebnis daraus könnte z. B. sein, dass ein Unternehmen feststellt, dass seine veraltete Firewall ein hohes Risiko darstellt – und dann als Gegenmaßnahme eine Modernisierung oder ein Managed Firewall Service beschließt.

b) Technische Sicherheitsmaßnahmen umsetzen:

NIS2 schreibt bestimmte Mindestmaßnahmen in der IT-Sicherheit vor, die implementiert sein müssen. Dazu gehören unter anderem:

Zugriffsschutz und Identitätsmanagement:
Prinzip der minimalen Rechte (Least Privilege), konsequente Nutzung von Multi-Faktor-Authentifizierung (MFA), klare Rollenkonzepte und Passwortrichtlinien.

Patch-Management und Schwachstellen-Management:
Regelmäßige Updates aller Systeme, zeitnahe Behebung bekannter Schwachstellen und proaktive Verwundbarkeits-Scans.

Protokollierung und Überwachung:
Zentrale Logfiles und Monitoring für sicherheitsrelevante Ereignisse, idealerweise in Echtzeit (hier kommt oft ein SIEM zum Einsatz – Security Information and Event Management)..

Verschlüsselung:
Schutz sensibler Daten sowohl bei der Speicherung (at rest) als auch bei der Übertragung (in transit) durch angemessene Kryptografie.

Netzwerk- und Systemsicherheit:
Netzwerksegmentierung, Firewalls, sichere Konfiguration der Systeme. Außerdem fortgeschrittene Endgerätesicherheit wie Endpoint Detection & Response (EDR) bzw. erweiterte Threat Detection (XDR) zur frühzeitigen Erkennung von Angriffsmus-tern.

Datensicherungen:
Zwar nicht explizit im Gesetzestext genannt, aber implizit notwendig: regelmäßige Backups, die gegen Ausfall und Ransomware geschützt sind (Offline-Backups, georedundant, getestet).

Diese Maßnahmen decken sich weitgehend mit etablierten Best Practices (z. B. ISO 27001-Kontrollen oder BSI-Grundschutz) – neu ist jedoch, dass ihre Umsetzung verbindlich vorgeschrieben wird.

c) Organisatorische Maßnahmen und Prozesse:

Neben Technik sind Prozesse entscheidend:

Vorfallmanagement (Incident Response): Es muss ein definierter Notfallplan existieren, wie das Unternehmen auf Sicherheitsvorfälle reagiert. Dazu gehören klar geregelte Eskalationsstufen (wer alarmiert wen bei einem größeren Cybervorfall?), vorbereitete Kommunikationspläne (intern und extern, z. B. an Behörden oder Medien) und regelmäßige Übungen bzw. Planspiele, um die Wirksamkeit zu testen. Ein gut ausgearbeitetes Incident Response Playbook kann im Ernstfall den Unterschied machen zwischen einem glimpflich abgewehrten Angriff und einem wochenlangen Stillstand.

Kontrolle von Drittparteien (Lieferketten): Die Sicherheit endet nicht an der eigenen Firewall. Unternehmen müssen sicherstellen, dass auch Dienstleister und Zulieferer angemessene Sicherheitsstandards einhalten. In der Praxis bedeutet dies: Sicherheitsanforderungen vertraglich festlegen (z. B. in Auftragsverarbeitungsverträgen oder SLA), regelmäßige Überprüfungen/Audits der wichtigsten Lieferanten (ggf. Fragebögen oder Zertifikate einfordern) und Einbeziehung von Drittparteien in die eigene Notfallplanung. Beispiel: Ein Maschinenbauer sollte prüfen, ob sein IT-Dienstleister alle Patch-Updates zeitnah einspielt, und im Vertrag ein schnelles Incident Reporting vereinbaren.

Schulung und Awareness: Mitarbeitende müssen regelmäßig geschult und sensibilisiert werden. Das umfasst grundlegende Cyber-Hygiene (Erkennen von Phishing, sicherer Umgang mit Passwörtern, Melden von Auffälligkeiten) und je nach Rolle vertiefte Trainings. Für Administratoren und IT-Personal sind z. B. weiterführende Schulungen Pflicht, da hier bei Fehlern großes Risiko besteht. Wichtig ist: Diese Schulungen müssen dokumentiert und nachweisbar sein (wer hat wann an welcher Unterweisung teilgenommen?) Awareness ist deshalb so kritisch, weil der Mensch oft das schwächste Glied der Kette ist – ein unachtsamer Klick kann hochentwickelte technische Schutzmaßnahmen aushebeln.

d) Dokumentation und Nachweispflichten:

Ein zentrales Prinzip von NIS2 ist „prüffähiger Nachweis". Unternehmen müssen ihre Cybersicherheitsmaßnahmen lückenlos dokumentieren und auf Verlangen der Aufsichtsbehörde (BSI) vorlegen können. Dies beinhaltet: IT-Sicherheitsrichtlinien, Rollen- und Verantwortlichkeitsbeschreibungen (z. B. wer ist IT-Sicherheitsbeauftragter, wer meldet Vorfälle ans BSI), Ergebnisberichte von Risikoanalysen, Inventar der technischen und organisatorischen Maßnahmen, Protokolle von Schulungen, Audit-Reports, Tests der Notfallpläne etc. Im Grunde verlangt NIS2 damit ein Informationssicherheits-Managementsystem (ISMS), wie man es etwa aus ISO 27001 kennt. Es muss kein ISO-Zertifikat erworben werden, aber die systematische Vorgehensweise ist vergleichbar. Gerade für mittelständische Unternehmen, die so etwas bisher nicht formal hatten, kann der Aufbau dieser Dokumentation eine Herausforderung sein – aber es ist nötig, um im Ernstfall gegenüber der Behörde die Compliance belegen zu können.

e) Meldepflicht bei Sicherheitsvorfällen:

Eine sehr konkrete Vorgabe von NIS2 ist die Meldepflicht bei erheblichen IT-Sicherheitsvorfällen. Wenn z. B. ein Angriff stattfindet, der die Dienstleistung erheblich beeinträchtigt (oder beeinträchtigen könnte), muss das Unternehmen dies dem BSI nach einem gestaffelten Zeitplan anzeigen:

> **Binnen 24 Stunden:**
Abgabe einer Frühwarnung bzw. Erstmeldung mit den vorläufig bekannten Fakten. (Das heißt, auch wenn noch nicht alles klar ist, soll sehr schnell eine Meldung rausgehen.)

> **Binnen 72 Stunden:**
Übermittlung einer weiteren Einschätzung / Zwischenberichts mit Ergebnissen der ersten Untersuchungen.

> **Binnen 1 Monat:**
Abgabe eines Abschlussberichts mit detaillierter Analyse des Vorfalls und ergriffenen Maßnahmen (in besonderen Fällen kann dieser Zeitraum verlängert werden).
Unterlässt ein Unternehmen diese Meldungen oder hält die Fristen nicht ein, drohen ebenfalls Sanktionen. Die Meldepflicht erfordert daher einen klar definierten Prozess intern: Mitarbeiter müssen wissen, welche Ereignisse meldepflichtig sind und sofort die IT/den CISO informieren. Verantwortliche müssen in der Lage sein, zügig einen Bericht ans BSI abzusetzen (es gibt dafür i.d.R. Formulare/Plattformen, wie z. B. das Meldeportal des BSI). Wichtig: Die Meldepflicht an die Behörde entbindet nicht davon, parallel alle notwendigen Schritte zur Schadensbegrenzung einzuleiten. NIS2 verlangt also ein professionelles Incident Management, das sowohl interne Bewältigung als auch externe Kommunikation umfasst.

Zusammengefasst fordert NIS2, dass Unternehmen proaktiv für Cybersicherheit sorgen und reaktiv professionell mit Vorfällen umgehen – und über alles Rechenschaft ablegen können. Für viele Mittelständler bedeutet das einen erheblichen Reifegrad-Sprung in Sachen IT-Sicherheit. Im nächsten Kapitel betrachten wir, welche konkreten Auswirkungen das für den Mittelstand hat und wo typische Stolpersteine liegen.

Was bedeutet NIS2 für den Mittelstand?

Herausforderungen und Chancen

Für mittelständische Unternehmen, die nun erstmals unter diese strengen Regulierungsvorgaben fallen, ist die Situation zweischneidig: Einerseits erzwingt NIS2 notwendige Investitionen in die Sicherheit, die langfristig das Unternehmen robuster machen. Andererseits stellen die Anforderungen viele Betriebe vor beträchtliche organisatorische und finanzielle Herausforderungen.

Ressourcenknappheit und Know-how:

Vielen KMUs fehlt es bereits heute an genügend IT-Sicherheits-Fachkräften. Ein eigenes Security Operations Center (SOC) rund um die Uhr zu betreiben oder laufend Risikoanalysen und Penetrationstests durchzuführen, sprengt oft die Möglichkeiten eines Mittelständlers. Die ohnehin überlasteten IT-Abteilungen müssen nun zusätzlich die Compliance-Aufgaben stemmen: Policies schreiben, Schulungen organisieren, Berichte an Behörden verfassen. Dies kann – insbesondere, wenn das Know-how intern begrenzt ist – schnell zur Überforderung führen.

Budget und Wirtschaftlichkeit:

IT-Sicherheit galt im Mittelstand leider oft als Kostenstelle ohne direkten Gegenwert. Nun müssen Budget und Mittel bereitgestellt werden für z. B. neue Security-Technologien

(etwa SIEM-System, EDR-Lösungen), externe Berater oder Schulungsprogramme. Zwar sind die möglichen Bußgelder (bis 10 Mio. €) und Schäden durch Cyberangriffe ein starkes Argument, um Budget locker zu machen, dennoch bleibt die Herausforderung, wirtschaftlich vertretbare Lösungen zu finden. Hier bieten sich oft Cloud- oder Managed-Services an, die skalierbar nach Bedarf genutzt werden können, statt hohe Einmalinvestitionen zu erfordern.

Bürokratie und Dokumentationsaufwand:

Eine häufige Sorge im Mittelstand sind die "Bürokratiekosten". Die NIS2-Pflichten zur Dokumentation, Auditierung und Nachweisführung bedeuten einen erheblichen administrativen Aufwand. Viele kleinere Unternehmen haben keine Compliance-Abteilung – oft bleibt diese Mehrarbeit an der IT-Leitung oder gar Geschäftsführung hängen. Es gilt also, pragmatische Wege zu finden, die geforderte Dokumentation zu erzeugen, ohne dass das Tagesgeschäft leidet. Hier können Standards und Vorlagen helfen (z. B. ein ISMS-Template oder Tools, die Dokumentationen halbautomatisch generieren).

Kulturwandel im Unternehmen:

NIS2 erfordert, dass Sicherheit zur Chefsache wird. Das Management muss nicht nur Mittel bereitstellen, sondern auch aktiv die Umsetzung vorantreiben und ein Sicherheitsbewusstsein im Unternehmen verankern. Das kann einen Kulturwandel bedeuten: Weg vom impliziten "IT macht das schon" hin zu Sicherheitsmanagement als Teil der Unternehmensführung. Mitarbeitende aller Ebenen müssen mitziehen – Security darf nicht mehr als lästige IT-Angelegenheit abgetan werden.

Zeitdruck und Übergangsfristen:

Da das deutsche Umsetzungsgesetz nun Ende 2025 in Kraft getreten ist, stellt sich die Frage: Bis wann müssen Unternehmen compliant sein? Theoretisch gilt das Gesetz ab sofort; praktisch dürfte es aber Übergangsfristen geben bzw. die Behörde wird eine gewisse Zeit zur Anpassung einräumen. Dennoch: Viel Zeit bleibt nicht, denn Cyberangriffe passieren jetzt und das BSI wird ab 2026 sicher die Einhaltung prüfen. Mittelständler stehen also unter Zeitdruck, schnell die wichtigsten Lücken zu schließen. Priorisierung ist hierbei das A und O.

Chancen durch NIS2:

Bei allem Mehraufwand – die Richtlinie birgt auch Chancen. Unternehmen, die jetzt ihre IT-Sicherheit auf Vordermann bringen, reduzieren ihr tatsächliches Risiko massiv. Ein erfolgreicher Cyberangriff kann heute katastrophale Folgen haben (Produktionsausfall, Datenschutzverletzungen, Imageverlust). Proaktives Handeln schützt vor solchen Schäden. Zudem kann Compliance auch zum Wettbewerbsvorteil werden: Wer nachweislich NIS2-konform ist, kann Kunden und Partnern gegenüber mit hoher Sicherheitsqualität punkten. In manchen Branchen werden Auftraggeber künftig verlangen, dass ihre Lieferanten NIS2 erfüllen – hier früh dabei zu sein schafft Vertrauen.

Synergien nutzen:

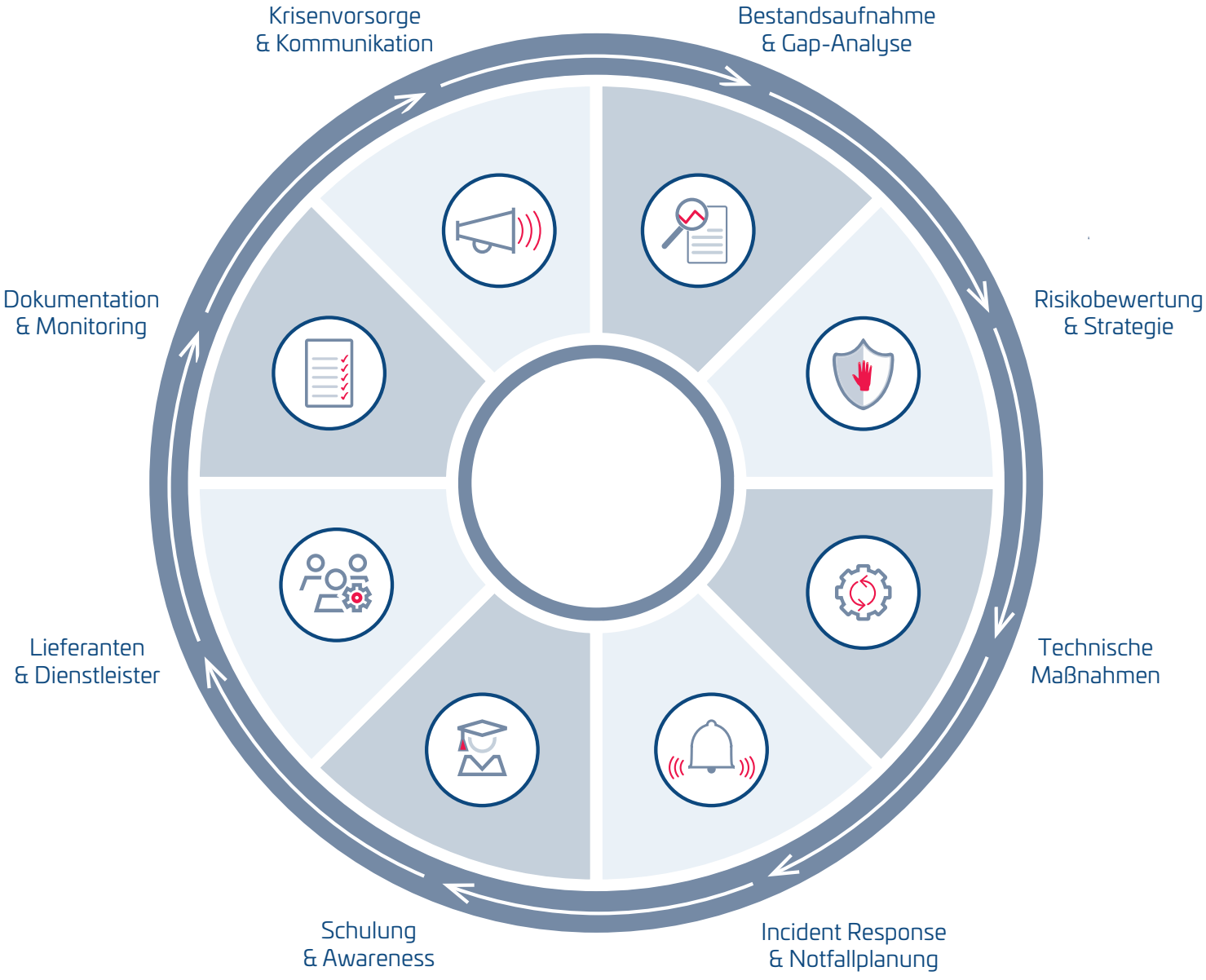
Viele NIS2-Anforderungen decken sich mit anderen Regelwerken (z. B. ISO 27001, TISAX in der Automobilindustrie, DSGVO beim Datenschutz). Mittelständler können Synergien heben, indem sie ein integriertes Managementsystem aufbauen, das mehrere Compliance-Themen gleichzeitig abdeckt. Beispielsweise überschneiden sich DSGVO und NIS2 bei Themen wie Datensicherheit und Meldepflicht (DSGVO-Notifikation von Datenpannen). Ein konzertierter Ansatz verhindert Doppelarbeit. In der behördlichen Praxis ist davon auszugehen, dass die Durchsetzung von NIS2 dem Grundsatz der Verhältnismäßigkeit folgt. Entscheidend ist jedoch, ob ein Unternehmen erkennbar und strukturiert an der Umsetzung arbeitet. Fehlende personelle oder finanzielle Ressourcen gelten ausdrücklich nicht als Entlastung. Unternehmen ohne dokumentierte Maßnahmen, klare Verantwortlichkeiten oder Umsetzungsplan riskieren frühzeitig aufsichtsrechtliche Maßnahmen – unabhängig davon, ob bereits ein Sicherheitsvorfall eingetreten ist. Unterm Strich zwingt NIS2 den Mittelstand dazu, IT-Sicherheit strategisch anzugehen – eine Aufgabe, die angesichts der Bedrohungslage ohnehin überfällig war. Damit die Umsetzung gelingt, empfiehlt es sich, strukturiert vorzugehen. Im nächsten Abschnitt stellen wir einen 8-Schritte-Plan vor, der als Richtschnur für die NIS2-Compliance dient.

Acht Schritte zur NIS2-Compliance

– Ein Fahrplan für Unternehmen

Der folgende 8-Schritte-Plan dient als praxisorientierte Roadmap für die Umsetzung der NIS2-Anforderungen im Mittelstand. Er orientiert sich sowohl an der NIS2-Richtlinie als auch an etablierten Standards wie ISO 27001 und dem BSI-Grundschutz. Ziel ist es, Geschäftsführung und IT-Verantwortlichen einen klar strukturierten Weg aufzuzeigen – unabhängig davon, ob die Umsetzung intern, extern oder hybrid erfolgt.

Die Umsetzung von NIS2 ist kein einmaliges Projekt, sondern ein kontinuierlicher Prozess. Dennoch lässt sich der Weg zur Compliance in klaren Etappen gliedern. Nachfolgend ein praxisbewährter 8-Schritte-Plan, der mittelständischen Unternehmen als Leitfaden dienen kann:



Schritt 1: Bestandsaufnahme und Gap-Analyse

Zunächst müssen Sie den Status quo Ihrer IT-Sicherheit verstehen. Führen Sie eine gründliche Bestandsaufnahme aller relevanten IT-Systeme, Daten und Prozesse durch. Welche Schutzmaßnahmen sind schon vorhanden, welche Richtlinien gibt es bereits? Legen Sie eine Soll-Ist-Analyse an: Stellen Sie den NIS2-Anforderungen (aus Abschnitt 4) systematisch gegenüber, was Ihr Unternehmen schon erfüllt und wo Lücken bestehen. Diese Gap-Analyse bildet die Basis für alle weiteren Schritte.
Idealerweise priorisieren Sie die identifizierten Lücken nach Risiko: Wo drohen akut große Gefahren oder Compliance-Verstöße? Beispiele: Vielleicht existiert bereits ein rudimentärer Notfallplan, aber es fehlen formale Schulungsnachweise und eine zentrale Protokollierung – dann wissen Sie, welche Punkte besonders anzugehen sind.

Schritt 2: Risikobewertung und Strategieplanung

Bauen Sie auf den Erkenntnissen auf und entwickeln Sie einen Plan. Durchlaufen Sie formal einen Risikomanagement-Prozess: Bewerten Sie die identifizierten Risiken nach Eintrittswahrscheinlichkeit und Schadensausmaß. Dieses Rating hilft, die Prioritäten festzulegen. Anschließend definieren Sie eine Cybersicherheitsstrategie bzw. einen Maßnahmenplan. Darin halten Sie fest, welche technischen, organisatorischen und personellen Maßnahmen bis wann umgesetzt werden sollen, um die NIS2-Konformität zu erreichen. Wichtig: Holen Sie die Geschäftsführung und alle relevanten Stakeholder ins Boot – die Strategie sollte von oben getragen und unterstützt werden. Setzen Sie auch Meilensteine: z. B. “Bis Ende Q2: Einführung MFA für alle Zugänge; bis Ende Q3: Incident Response Plan fertig; fortlaufend: monatliche Phishing-Tests” etc.

Schritt 3: Implementierung technischer Maßnahmen

Jetzt geht es an die praktische Umsetzung der geplanten Verbesserungen. Viele Maßnahmen betreffen die IT-Infrastruktur. Beispiele: Implementieren Sie flächendeckend Multi-Faktor-Authentifizierung für VPN, E-Mail und kritische Anwendungen, falls noch nicht geschehen (dies adressiert einen Großteil der Angriffe durch kompromittierte Passwörter). Richten Sie eine zentrale Log-Management-Lösung oder ein SIEM ein, um Anomalien zu erkennen. Aktualisieren Sie Firewalls und segmentieren Sie Ihr Netzwerk, damit Angreifer sich nicht lateral ausbreiten können. Führen Sie ein Vulnerability Management ein, inklusive regelmäßiger Schwachstellen-Scans und definierter Patch-Zeitfenster. Falls Ressourcen fehlen, ziehen Sie externe Hilfe in Betracht – etwa einen Dienstleister, der monatliche Penetrationstests durchführt, oder einen Managed Service für 24/7-Monitoring. Achten Sie darauf, die eingeführten Lösungen sauber zu dokumentieren (Konfigurationen, Verantwortliche, Wartungsintervalle etc.), da dies später für den Nachweis wichtig ist.

Schritt 4: Aufbau von Incident-Response- und Notfallprozessen

Parallel zur Prävention muss auch die Reaktion vorbereitet sein. Erarbeiten Sie einen Notfallplan für Cybervorfälle: Wer befindet sich im Incident Response Team? (z. B. IT-Leiter, CISO, PR-Verantwortlicher, ggf. Geschäftsführung). Welche Alarmierungsketten gibt es bei einem schweren Sicherheitsvorfall nachts oder am Wochenende? Definieren Sie konkrete Maßnahmen für verschiedene Szenarien: z. B. Ransomware-Befall – Server vom Netz nehmen, Backups prüfen, Forensiker hinzuziehen, Anwaltskanzlei und Polizei informieren etc. Legen Sie fest, wer an das BSI meldet und wie die Fristen eingehalten werden. Diese Prozesse schreibt man idealerweise als Handbuch oder Ablaufdiagramm nieder. Testen Sie den Ernstfall in regelmäßigen Abständen: Einmal pro Jahr ein Simulationstest (Table-Top-Übung) hilft, Lücken im Plan aufzudecken und Mitarbeiter mit den Abläufen vertraut zu machen. Solche Übungen sollten ebenfalls dokumentiert werden (Datum, Teilnehmer, Lessons Learned).

Schritt 5: Sensibilisierung und Schulung der Mitarbeiter

Menschen sind eine entscheidende Verteidigungslinie. Etablieren Sie ein kontinuierliches Security Awareness Programm.

Dazu gehört: Alle Mitarbeiter durchlaufen mindestens einmal jährlich ein Training zu grundlegenden Cybergefahren (Phishing, Social Engineering, sichere Passwörter, Umgang mit externen Datenträgern etc.). Spezifische Rollen – z. B. Administratoren, Entwickler – erhalten vertiefende Schulungen zu ihren Themen (sichere Konfiguration, sicherer Programmiercode, Incident Handling). Neue Mitarbeiter erhalten im Onboarding direkt eine Sicherheitseinweisung. Nutzen Sie e-Learning-Plattformen oder regelmäßige Phishing-Simulationen, um das Bewusstsein hoch zu halten. Und ganz wichtig: Dokumentieren Sie jede Schulung – wer (Name, Abteilung) hat wann welche Inhalte gelernt und die Prüfung bestanden? So können Sie im Auditfall sofort nachweisen, dass Sie der Schulungspflicht nachgekommen sind.

Schritt 6: Lieferanten und Dienstleister einbinden

NIS2-Compliance endet nicht an der eigenen Bürotür. Überprüfen Sie Ihre kritischen Dienstleister: Haben Sie IT-Dienstleister, Cloud-Provider, externe Rechenzentren, Logistikpartner, deren Ausfall Sie lahmlegen würde? Stellen Sie sicher, dass in Verträgen Sicherheitsanforderungen verankert sind (z. B. Mindest-Standards, Meldepflicht bei Vorfällen, ggf. Zertifizierungen). Fordern Sie Nachweise ein – etwa ISO 27001-Zertifikate oder Eigenerklärungen zur IT-Sicherheit. Eventuell müssen bestehende Verträge nachgebessert werden, um NIS2 gerecht zu werden. Führen Sie für die wichtigsten Lieferanten ein Risikoassessment durch[30]: Welche Risiken gehen von ihnen aus und welche Kontrollen sind vorhanden? Dokumentieren Sie diese Third-Party Risk Assessments. Auch interne Prozesse wie Einkaufs- und Onboarding-Prozesse sollten angepasst werden: Sicherheitskriterien müssen bei der Auswahl neuer Anbieter eine Rolle spielen. Kurz: Schaffen Sie Transparenz und Einfluss über Ihre Supply Chain, damit dort kein verborgenes Einfallstor klafft.

Schritt 7: Dokumentation und kontinuierliches Monitoring

Nachdem die Haupt-Maßnahmen umgesetzt sind, geht es nun um nachhaltige Verankerung. Richten Sie ein IT-Sicherheitshandbuch oder ISMS ein, in dem alle Policies, Prozesse und Verantwortlichkeiten schriftlich festgehalten sind. Führen Sie regelmäßige Audits oder Reviews durch – z. B. vierteljährliche Management-Reviews der Sicherheitslage, jährliche interne Audits zu bestimmten Controls. Überwachen Sie laufend Ihre Infrastruktur: Ein Security Operations Center (intern oder extern betrieben) kann z. B. täglich Alerts auswerten. Kennzahlen (KPIs) helfen beim Monitoring, z. B.: Anzahl kritischer Schwachstellen mit Patch-Zeit >30 Tage, Zeit bis zur Konto-Sperrung nach Mitarbeiteraustritt, Phishing-Click-Rate in Tests etc. Diese Messgrößen zeigen, ob Ihre Maßnahmen wirken oder justiert werden müssen. Wichtig ist auch, immer die Aktualität zu bewahren: Bedrohungslage und Technologien ändern sich, also gehören Updates der Sicherheitsstrategie und der Maßnahmen zum kontinuierlichen Verbesserungsprozess dazu.

Schritt 8: Vorbereitung auf den Ernstfall und externe Kommunikation

Der letzte Schritt schließt den Kreis und stellt sicher, dass Sie in brenzligen Situationen handlungsfähig bleiben. Etablieren Sie eine Krisenkommunikation: vorbereitete Stellungnahmen, falls ein Vorfall öffentlich wird, und definierte Sprecherrollen (z. B. nur Geschäftsführer oder PR sprechen mit Presse). Prüfen Sie Ihre Versicherungen – Cyber-Versicherungen können finanzielle Schäden abfedern, aber oft nur, wenn bestimmte Sicherheitsmaßnahmen nachweislich vorhanden waren (Compliance hilft hier). Halten Sie einen ständigen Verbesserungsprozess aufrecht: Nach jedem größeren Zwischenfall (oder auch Übung) führen Sie eine Nachbesprechung durch: Was lief gut, was schlecht? Passen Sie Prozesse entsprechend an. Und sorgen Sie dafür, dass Ihre NIS2-Dokumentation immer aktuell ist, damit bei einer Prüfung durch das BSI alles parat liegt.

Dieser 8-Stufen-Plan hilft, nichts Wesentliches zu vergessen, und strukturiert die Reise zur Compliance. Natürlich ist jedes Unternehmen anders – die Schritte können in der Praxis teilweise parallel ablaufen oder müssen iterativ verfeinert werden. Wichtig ist vor allem, den Anfang zu machen und Schritt für Schritt voranzugehen. Viele Mittelständler werden feststellen, dass sie nicht alle Aufgaben alleine bewältigen können oder wollen. Hier lohnt es sich, über externe Unterstützung nachzudenken – das führt uns zum nächsten Kapitel.

Make-or-Buy:

NIS2-Umsetzung intern stemmen oder mit Partner?

Angesichts der umfangreichen Anforderungen stellt sich vielen mittelständischen Unternehmen die Frage: Welche Aufgaben können wir selbst leisten, und wo brauchen wir Unterstützung? Die Entscheidung Make-or-Buy ist in der IT-Sicherheit zentral, da Fachkräfte knapp und Budgets begrenzt sind. Hier einige Überlegungen dazu:

Make or Buy

Intern:

- Kontrolle im Haus
- Hoher Personalbedarf
- Know-how nötig
- Begrenzte Skalierung

Extern (MSSP):

- 24/7 Monitoring
- Espertenwissen
- Planbare Kosten
- Entlastung der IT

Interne Umsetzung – Was spricht dafür?

Wenn ein Unternehmen bereits eine versierte IT- oder Security-Abteilung hat, kann es attraktiv sein, das Know-how intern aufzubauen. Man behält die volle Kontrolle über Daten und Prozesse. Manche Maßnahmen, wie z. B. die Entwicklung von Sicherheitsrichtlinien oder das Durchführen von Mitarbeiterschulungen, lassen sich mit etwas Aufwand intern entwickeln – zumal es mittlerweile viele freie Ressourcen und Vorlagen gibt. Ein weiterer Punkt: Branchenspezifisches Wissen (z. B. besondere Produktionsanlagen) ist oft intern besser vorhanden und nötig, um die richtigen Sicherheitsprioritäten zu setzen.

Interne Umsetzung – Grenzen und Risiken:

Die Realität zeigt, dass vielen mittelständischen Firmen die personellen Ressourcen fehlen, um z. B. ein 24/7 Monitoring oder aufwändige forensische Analysen im Ernstfall intern zu betreiben. Cybersecurity ist ein komplexes Feld; die Bedrohungen entwickeln sich ständig weiter. Es ist schwierig und teuer, Mitarbeiter in allen benötigten Spezialbereichen (Malware-Analyse, Cloud-Security, Incident Response etc.) fit zu machen – insbesondere, wenn die Unternehmensgröße das nicht hergibt. Zudem kann es intern zu Interessenkonflikten kommen: Das IT-Team hat auch noch den operativen Betrieb am Laufen und kann Sicherheitsprojekte nicht voll priorisieren. Die Folge könnten Verzögerungen oder halbherzige Implementierungen sein.

Externe Unterstützung durch Dienstleister – Was ist möglich?

Hier kommt der Ansatz der Managed Security Services ins Spiel. Ein Managed Security Service Provider (MSSP) übernimmt bestimmte Sicherheitsaufgaben im Auftrag des Unternehmens. Typische Leistungen sind z. B.: Betrieb eines Security Operations Center (SOC) mit 24/7-Überwachung, Bereitstellung eines SIEM-Systems inklusive Use-Case-Entwicklung, Managed Firewall und Netzwerkschutz, Endpoint Security als Service, Vulnerability Management, Incident Response Unterstützung bis hin zur Bereitstellung

von Security Awareness Trainings. Auch das komplette Compliance-Management (d.h. Aufbau und Pflege des ISMS) lässt sich teilweise outsourcen, zumindest beratend begleiten.

Der Vorteil: Ein MSSP beschäftigt Expertenteams, die sich rund um die Uhr nur mit Sicherheit befassen. Sie nutzen modernste Technologien und erfahrene Analysten, was einem einzelnen Mittelständler so kaum möglich wäre. Dadurch können Angriffe frühzeitig erkannt und abgewehrt werden, oft bevor sie größeren Schaden anrichten. Außerdem entlastet es die eigene IT, die sich weiterhin auf das Kerngeschäft und die IT-Basisservices konzentrieren kann. Finanziell kann es ebenfalls sinnvoll sein: Ein externer Service mit definierter monatlicher Rate ist planbar und meist günstiger als eigene Security-FTEs inklusive 24/7-Schichtbetrieb einzustellen.

Worauf achten beim Outsourcing?

Natürlich gibt man mit externen Partnern einen Teil der Verantwortung aus der Hand – wobei man die Verantwortung nach NIS2 nie vollständig delegieren kann. Die Geschäftsleitung bleibt accountable, aber man kann sich einen sachkundigen Erfüllungsgehilfen suchen. Wichtig ist, in Verträgen mit MSSPs klare Service Level Agreements (SLAs) zu definieren (z. B. Reaktionszeit im Incident, Verfügbarkeit des SOC, Reporting-Intervalle). Auch sollte geregelt sein, wie der Austausch mit dem BSI läuft – im Ernstfall muss eventuell der Dienstleister schnell Zuarbeit für die Meldung liefern. Ein weiterer Aspekt: Datenschutz und Zugriffsrechte. Ein MSSP wird tiefen Einblick in die Systeme haben; hier ist Vertrauen und entsprechende Vertragsgestaltung (z. B. Geheimhaltung, Auftragsverarbeitung) essenziell.

Fazit:

Viele mittelständische Unternehmen werden eine Hybrid-Strategie wählen. Das heißt: Kernkompetenzen und Hoheit über kritische Entscheidungen bleiben intern (z. B. Risikobeurteilung, Sicherheitsstrategie, Kommunikation mit Behörden), während operative Aufgaben („Security Operations“) ganz oder teilweise ausgelagert werden. Beispielsweise kann man das Monitoring und die initiale Incident Response einem Dienstleister übergeben, behält aber das Patch-Management und die Schulungen inhouse. Entscheidend ist, einen Partner zu finden, der die besonderen Anforderungen des Mittelstands versteht – pragmatisch, bezahlbar, aber dennoch auf hohem professionellem Niveau.

Im nächsten Kapitel stellen wir die SpaceNet AG als einen solchen Partner vor und zeigen anhand eines konkreten Praxisbeispiels, wie ein mittelständisches Unternehmen durch Zusammenarbeit mit SpaceNet seine NIS2-Compliance erfolgreich erreicht hat.

SpaceNet als Partner für NIS2-Compliance –
Managed Security in der Praxis

Als langjähriger IT-Dienstleister und Managed Security Service Provider bietet SpaceNet speziell für mittelständische Kunden umfassende Unterstützung auf dem Weg zur NIS2-Compliance. Im Folgenden schildern wir ein Praxisbeispiel, wie SpaceNet einem mittelständischen Unternehmen geholfen hat, die neuen Vorgaben effizient umzusetzen:

Ausgangssituation:

Ein mittelständisches Fertigungsunternehmen (ca. 300 Mitarbeiter) sah sich Anfang 2025 mit den neuen Compliance-Vorgaben der NIS2-Richtlinie konfrontiert. Die regulatorischen Anforderungen an IT-Sicherheit und Resilienz hatten sich deutlich verschärft, was das Unternehmen zwang, seine bisherige Sicherheitsstrategie zu überdenken. Die vorhandenen IT-Ressourcen waren bereits

stark ausgelastet mit dem Tagesgeschäft, und es fehlte an spezialisiertem Know-how, um komplexe Cyber-Bedrohungen effektiv abzuwehren und gleichzeitig den neuen gesetzlichen Vorgaben gerecht zu werden. Die Geschäftsführung machte zur Auflage, dass der interne Aufwand für die IT möglichst minimal bleiben müsse – das Unternehmen wollte sich weiterhin auf sein Kerngeschäft (Maschinenbau) konzentrieren können und keine große eigene Security-Organisation aufbauen.

Die Lösung: SpaceNet als Managed Security Service Provider (MSSP)

Nach einer intensiven Beratung entschied man sich, SpaceNet als externen Partner zu beauftragen, um die Sicherheitsarchitektur zu optimieren und die NIS2-Compliance-Anforderungen effizient umzusetzen. SpaceNet schnürte ein individuelles Maßnahmenpaket, das eng mit der IT-Leitung des Unternehmens abgestimmt wurde. Eine zentrale Rolle spielte dabei das SpaceNet Security Operations Center (SOC), welches rund um die Uhr (24/7) Bedrohungen analysiert und abwehrt.

Zunächst führte SpaceNet gemeinsam mit dem Kunden eine Initialanalyse der bestehenden IT-Infrastruktur und Sicherheitsmaßnahmen durch (vergleichbar mit Schritt 1 und 2 aus dem vorherigen Kapitel). Daraufhin wurde ein auf den Kunden zugeschnittenes Sicherheitskonzept entwickelt, das folgende Kernkomponenten umfasste:

SpaceNet SOC:

Eine 24/7-Überwachung der IT-Systeme des Kunden sowie kontinuierliche Bedrohungsanalysen, um Angriffe frühzeitig zu erkennen und zu stoppen[46]. Konkret richtete SpaceNet Sensoren und Log-Forwarder in der Kundeninfrastruktur ein, die sicherheitsrelevante Ereignisse in Echtzeit an das zentrale SOC melden. Dort beobachten erfahrene Analysten und KI-gestützte Systeme rund um die Uhr die Lage. Bei Auffälligkeiten (z. B. ein ungewöhnlicher Login nachts oder ein verdächtiges Datenmuster) wird sofort reagiert

Managed SIEM:

Die Implementierung eines Security Information and Event Management (SIEM)-Systems, betrieben durch SpaceNet[47]. Dieses System sammelte Logs von Servern, Firewalls, Anwendungen und Endgeräten des Kunden und führte Korrelationen durch, um mögliche Angriffe aufzudecken. SpaceNet übernahm die komplette SIEM-Infrastruktur als Service, inklusive Regelwerk-Updates und Alarmierung. Dadurch erhielt der Kunde praktisch eine Echtzeit-Analyse seiner Sicherheitsereignisse, ohne selbst eine komplexe SIEM-Umgebung aufbauen zu müssen.

Endpoint Detection & Response (EDR):

Einführung einer fortschrittlichen Endgerätesicherheit auf allen Clients und Servern[48]. SpaceNet verteilte einen EDR-Agent auf die Endpoints des Kunden. Diese Lösung, unterstützt durch KI, erkannte verdächtiges Verhalten (z. B. unbekannte Prozesse, Datei-Verschlüsselungen) auf den Rechnern und konnte automatisiert Gegenmaßnahmen ergreifen. So waren die Arbeitsplätze und Produktionssysteme des Kunden besser vor Ransomware und anderer Malware geschützt.

Security Awareness Training:

SpaceNet unterstützte beim Aufbau eines Schulungsprogramms für die Mitarbeiter. Dies umfasste E-Learning-Module, regelmäßige Phishing-Testkampagnen und Workshops vor Ort. Ziel war es, die Belegschaft als menschliche Firewall zu stärken, damit Social-Engineering-Angriffe ins Leere laufen. Durch SpaceNets Erfahrung konnten die Inhalte praxisnah und kurzweilig gestaltet werden, was die Akzeptanz im Betrieb förderte.

Compliance-Management und Beratung:

Parallel zu den technischen Maßnahmen stellte SpaceNet sicher, dass die Erfüllung der NIS2-Vorgaben kontinuierlich geprüft und dokumentiert wurde[50]. Ein dedizierter Security Consultant von SpaceNet fungierte quasi als externer ISMS-Beauftragter für den Kunden. Er half bei der Erstellung der notwendigen Richtlinien (z. B. Informationssicherheitsleitlinie, Incident-Response-Plan), führte interne Audits durch und bereitete die Reports für das Management und ggf. für das BSI vor. Somit hatte der Mittelständler jederzeit den Überblick, wo er auf seiner Compliance-Reise steht. Ergebnis und Mehrwert: Dank der Zusammenarbeit mit SpaceNet konnte das Unternehmen in kurzer Zeit folgende Erfolge verbuchen:

Verbesserte Sicherheitslage:

Durch die 24/7-Überwachung und die neuen Schutzmechanismen wurden Cyberangriffe nun frühzeitig erkannt und abgewehrt. Bereits im ersten Monat entdeckte das SpaceNet SOC mehrere verdächtige Aktivitäten (u. a. einen gezielten Phishing-Versuch auf Führungskräfte), die rasch eingedämmt wurden, bevor Schaden entstand.

Entlastung der internen IT:

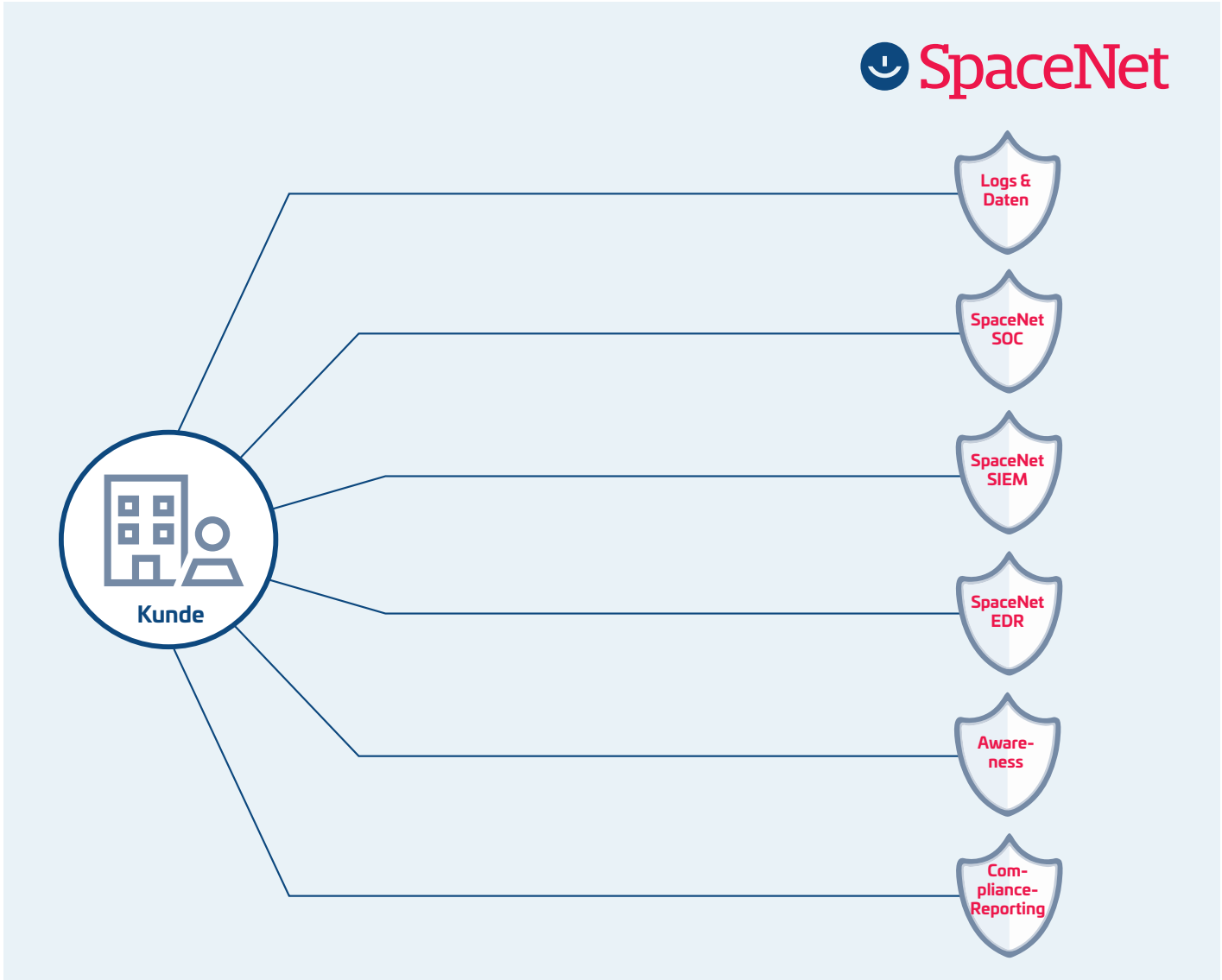
Viele Routine-Aufgaben der IT-Sicherheit lagen nun bei SpaceNet. Das eigene IT-Team wurde deutlich entlastet, da z. B. nächtliche Alarmmeldungen und Log-Analysen komplett vom SpaceNet SOC übernommen wurden. Die internen Mitarbeiter konnten sich wieder vermehrt ihren Kernaufgaben (Netzwerk-Betreuung, ERP-System etc.) widmen, ohne Angst zu haben, wichtige Sicherheitsvorfälle zu verpassen.

Nahtlose Erfüllung der NIS2-Compliance

Mit SpaceNets Unterstützung erfüllte der Kunde alle neuen NIS2-Vorgaben fristgerecht, ohne in eine Bürokratiefalle zu tappen[55]. Die laufenden Audits und Dokumentationen seitens SpaceNet stellten sicher, dass im Fall einer BSI-Prüfung alle Nachweise bereitliegen. Insbesondere die Meldewege wurden gemeinsam getestet, sodass das Unternehmen in der Lage ist, einen Vorfall innerhalb der 24-Stunden-Frist qualifiziert zu melden.

Kontinuierliche Verbesserung der Sicherheit:

Die Sicherheitsmaßnahmen des Kunden sind jetzt kein statisches Projekt mehr, sondern befinden sich im kontinuierlichen Verbesserungsprozess. SpaceNet führt regelmäßig Schwachstellenanalysen durch, passt das Regelwerk des SIEM an neue Bedrohungen an und berät zu neuen Best Practices (etwa dem Einsatz von Zero-Trust-Ansätzen). All das geschieht, ohne dass der Kunde hohe Investitionen in eigene Security-Teams oder Infrastruktur tätigen muss.



Fokus auf Kerngeschäft:

Letztlich ermöglichte die Partnerschaft dem Mittelständler, sich voll auf seine eigentliche Geschäftstätigkeit – die hochwertige Fertigung – zu konzentrieren, während Security und Compliance in den Händen von Experten lagen[58]. Die Geschäftsführung schlief ruhiger, wissend, dass ein wachsames Security-Team ständig über die IT wacht und im Ernstfall sofort eingreift.

Dieses Beispiel zeigt, wie ein mittelständisches Unternehmen die Herausforderung NIS2 erfolgreich meistern kann, indem es externes Fachwissen sinnvoll einbindet. SpaceNet tritt hierbei nicht als bloßer Lieferant auf, sondern als Partner auf Augenhöhe, der die spezifischen Bedürfnisse und Bedingungen des Mittelstands versteht. Leistungen wie Managed SOC, Managed SIEM, EDR, Awareness-Programme und Compliance-Beratung greifen ineinander und ergeben ein rundes Gesamtpaket.

Natürlich ist jede Unternehmenssituation anders – SpaceNet entwickelt daher für jeden Kunden ein maßgeschneidertes Konzept. Ob Sie nur punktuell Unterstützung brauchen (z. B. einmalige Beratung oder eine bestimmte technische Lösung) oder einen kompletten Managed Security Service: Wichtig ist, frühzeitig die richtigen Partner ins Boot zu holen, um die NIS2-Compliance rechtzeitig und effizient zu erreichen.

Fazit und nächste Schritte

Fazit

Die NIS2-Richtlinie markiert den Beginn einer neuen Ära in der IT-Sicherheit für mittelständische Unternehmen. Cybersicherheit ist nicht länger nur eine technische Frage für die IT-Abteilung, sondern eine strategische Führungsaufgabe. Geschäftsleitungen werden in die Pflicht genommen, und das zu Recht: Angesichts der allgegenwärtigen Cyber-Bedrohungen – vom Datendiebstahl bis zur Betriebsstilllegung durch Ransomware – hängt der Unternehmenserfolg und -ruf heute unmittelbar von einer robusten Sicherheitsstrategie ab.

In diesem Whitepaper haben wir die Relevanz von NIS2 für den Mittelstand herausgearbeitet und die wichtigsten Pflichten verständlich gemacht. Viele Leser werden sich darin wiedererkennen: Die Anforderungen sind hoch, aber sie sind machbar. Wer sich strukturiert vorbereitet – etwa entlang des hier vorgestellten 8-Schritte-Fahrplans – kann die Weichen rechtzeitig stellen. Dabei zahlt sich jeder investierte Euro doppelt aus: Er steigert nicht nur die Compliance, sondern auch den tatsächlichen Schutz vor Angriffen.

Wichtig ist, die Aufgabe jetzt aktiv anzugehen. Warten Sie nicht, bis das BSI anklopft oder – schlimmer – ein schwerer Sicherheitsvorfall Sie zum Handeln zwingt. Erste Schritte können sofort eingeleitet werden, zum Beispiel: Identifizieren Sie, ob Ihr Unternehmen unter NIS2 fällt (wenn Sie es nicht schon wissen). Sensibilisieren Sie die Geschäftsleitung mit den Kernpunkten der Richtlinie und den potenziellen Haftungsrisiken. Fangen Sie an, ein Kernteam oder Verantwortliche für die NIS2-Umsetzung zu benennen.

Scheuen Sie sich nicht, externe Hilfe hinzuzuziehen. Wie gezeigt, kann die Zusammenarbeit mit einem Partner wie SpaceNet den Weg zur Compliance erheblich erleichtern. Ein erfahrener Dienstleister bringt Best Practices mit, kennt Fallstricke und kann Lösungen oft schneller implementieren, als wenn man bei Null anfangen muss. Gerade für mittelständische Unternehmen, die keine großen Sicherheitsstäbe aufbauen wollen, sind Managed Security Services eine attraktive Option, um Sicherheit einzukaufen, ohne die Kontrolle zu verlieren.

Als nächste Schritte empfehlen wir:

NIS2-Quick-Check durchführen:

Lassen Sie Ihr Unternehmen durch einen kurzen Audit oder Fragebogen bewerten, wo Sie in Bezug auf NIS2 stehen. SpaceNet bietet beispielsweise einen NIS2-Check an, bei dem die wichtigsten Punkte durchgegangen werden und Sie einen Report mit Handlungsempfehlungen erhalten. Dieses low-cost/low-commitment Angebot kann einen guten Einstieg bilden.

Kontakt aufnehmen für eine Beratung:

Jedes Unternehmen hat individuelle Gegebenheiten. Eine persönliche Beratung – ob durch SpaceNet oder einen anderen vertrauenswürdigen Sicherheitsexperten – kann klären, welche Umsetzungsschritte bei Ihnen Priorität haben und wie ein Projektplan aussehen könnte. Oft hilft es schon, im Rahmen eines Workshops die Verantwortlichkeiten und Timeline grob abzustecken.

Awareness im Unternehmen schaffen:

Kommunizieren Sie intern, dass NIS2 kommt und was es bedeutet. Holen Sie Führungskräfte und Schlüsselpersonen ins Boot. Vielleicht versenden Sie ein Infoblatt oder veranstalten einen kurzen Kick-off. Die Umsetzung wird umso reibungsloser laufen, je mehr Akzeptanz und Verständnis im Unternehmen herrscht.

Zum Abschluss lässt sich festhalten:

NIS2 ist Herausforderung und Chance zugleich. Der mittelständische Wirtschaftsstandort Deutschland kann durch höhere Cyber-Resilienz insgesamt profitieren. Ja, es erfordert Investitionen und Mühe – aber der Schutz von Daten, Geschäftsgeheimnissen und Produktionsprozessen war noch nie so wichtig wie heute. Unternehmen, die jetzt handeln, werden langfristig sicherer, vertrauenswürdiger und wettbewerbsfähiger aufgestellt sein.

SpaceNet steht Ihnen hierbei gerne als kompetenter Partner zur Seite, mit technischem Know-how, pragmatischer Beratung und Services, die genau auf den Mittelstand zugeschnitten sind. Zögern Sie nicht, uns für einen unverbindlichen Austausch oder unseren NIS2-Check zu kontaktieren. Gemeinsam machen wir Ihr Unternehmen fit für die Anforderungen der NIS2 – und damit ein gutes Stück sicherer. (Kontaktinformationen und weiterführende Quellen finden Sie im Anhang.)

Anhang

Glossar

> **BSI (Bundesamt für Sicherheit in der Informationstechnik):**
Nationale Behörde in Deutschland zuständig für Cyber-Sicherheit, u. a. Aufsichtsbehörde für NIS2-Umsetzung in betroffenen Unternehmen.

> **EDR (Endpoint Detection & Response):**
Sicherheitslösung, die Endgeräte (PCs, Server) kontinuierlich auf verdächtige Aktivitäten überwacht und bei Anomalien reagiert. Soll fortgeschrittene Angriffe erkennen, die herkömmliche Virenscanner verpassen.

> **Incident Response (Vorfallreaktion):**
Geplanter Prozess zur Reaktion auf IT-Sicherheitsvorfälle. Beinhaltet Erkennung, Eindämmung, Behebung und Nachbereitung eines Angriffs nach definierten Abläufen.

>

> **ISMS (Information Security Management System):**
Managementsystem für Informationssicherheit, das Policies, Prozesse, Verantwortlichkeiten und Maßnahmen umfasst. Zielt auf kontinuierliche Verbesserung der Sicherheit ab (bekanntestes Beispiel: ISO 27001).

> **ISO 27001:**
International anerkannte Norm für Informationssicherheits-Managementsysteme. Hilft dabei, systematisch die Informationssicherheit im Unternehmen zu steuern. NIS2 fordert kein ISO-27001-Zertifikat, orientiert sich aber inhaltlich daran.

> **IT-Grundschutz:**
Ein vom BSI entwickeltes Rahmenwerk mit Standardsicherheitsmaßnahmen und Katalogen. Hilft vor allem deutschen Behörden und Unternehmen, ein Basis-Sicherheitsniveau umzusetzen. Kann für NIS2 als Hilfsmittel dienen.

> **Kritis:**
Abkürzung für kritische Infrastrukturen. Gemeint sind Organisationen aus Sektoren, die für das Gemeinwesen essenziell sind (Energie, Wasser, Ernährung, Gesundheit, Finanzen, Transport etc.). Unter NIS2 nun teilweise als BWE bezeichnet.

> **Meldepflicht:**
Die Verpflichtung, erhebliche IT-Sicherheitsvorfälle an eine Behörde (in DE: BSI) zu melden. Unter NIS2 streng geregelt mit gestaffelten Fristen (24h, 72h, 30 Tage).

> **MFA (Multi-Faktor-Authentifizierung):**
Zusätzlicher Sicherheitsnachweis bei Login neben Passwort, z. B. Einmalcode per App/SMS oder Hardware-Token. Erschwert das missbräuchliche Nutzen gestohlener Passwörter erheblich.

> **•MSSP (Managed Security Service Provider):**
Externer Dienstleister, der für Kunden Teile der IT-Sicherheit managt (z. B. Security Monitoring, Betrieb von Firewalls, Incident Response Unterstützung, etc.). Bietet Expertise und oft 24/7-Dienste, die intern nur schwer aufzubauen wären.

> **NIS2:**
Zweite EU-Richtlinie über Netz- und Informationssicherheit. Vollständiger Name: Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union. Rechtsakt, der Mitgliedstaaten Vorgaben für Cybersicherheitsanforderungen in bestimmten Unternehmen macht.

> **NIS2-Umsetzungsgesetz:**
Deutsches Gesetz zur Umsetzung der NIS2-Richtlinie (voller Name: Gesetz zur Umsetzung der Richtlinie (EU) 2022/2555 und zur Stärkung der Cybersicherheit). Konkretisiert in Deutschland, welche Unternehmen betroffen sind und wie die NIS2-Vorgaben angewendet werden.

> **Patch-Management:**
Prozess, um Softwareupdates und Sicherheits-Patches zeitnah einzuspielen. Kritisch, um bekannte Schwachstellen zuschließen, bevor Angreifer sie ausnutzen.

> **Penetrationstest:**
Simulierter Angriff durch Sicherheitsspezialisten, um Schwachstellen in IT-Systemen aufzudecken. Hilft Unternehmen, Lücken zu finden, bevor echte Angreifer diese entdecken.

> **SIEM (Security Information and Event Management):**
Zentralisiertes System, das Log-Daten aus diversen Quellen sammelt und analysiert, um Anzeichen von Sicherheitsvorfällen zu erkennen. Oft Kern eines SOC, mit Korrelationsregeln und Alarmierungsmechanismen.

> **SOC (Security Operations Center):**
Zentrale Einheit (Team und technologische Plattform) zur Überwachung der IT-Sicherheitslage eines Unternehmens in Echtzeit. Ein SOC reagiert auf Alarmmeldungen, analysiert Vorfälle und koordiniert Gegenmaßnahmen – idealerweise 24/7.

Quellenverzeichnis

> **Bitkom-Studie "Wirtschaftsschutz 2024"**
Zahlen zu Cyberangriffen auf Unternehmen (81 % betroffen, Schäden 266 Mrd. €).

> **SpaceNet White Paper "Cybersicherheit im Fokus: Wie MSSP den Mittelstand effektiv schützen können"**
Auszüge zum Anstieg der Bedrohungslage und der Rolle von MSSPs sowie Praxisbeispiel SpaceNet als MSSP.

> **EU-Richtlinie 2022/2555 (NIS2)**
Offizieller EU-Rechtsakt, veröffentlicht am 27. Dezember 2022 (ABl. L 333). Kernforderungen zusammengefasst in Abschnitt 4 dieses Whitepapers, insbesondere zu Risikomanagement, Maßnahmen und Meldepflichten.

> **IITR Datenschutz GmbH: "NIS-2 in Deutschland: Was Unternehmen jetzt tun müssen**
kompakter Leitfaden für Entscheider" (Blogbeitrag vom 25. 11. 2025) – Wichtige Informationen zu betroffenen Unternehmen und Pflichten, inklusive Kategorien BWE/WE und Schwellenwerte.

> **BVMW Stellungnahme (07/2025) zum Referentenentwurf NIS2-Umsetzungsgesetz**
Hinweis auf Herausforderungen für den Mittelstand (Bürokratiekosten, Lieferkettenanforderungen).

> **DIHK Meldung (Dez 2025)**
Bestätigung Inkrafttreten des NIS2-Umsetzungsgesetzes am 5. Dezember 2025[18].

> **All About Security (15. Dez 2025)**
Kritischer Artikel "So wird NIS-2 zu Nichts-2" über Verzögerungen in der deutschen Umsetzung (zeigt zeitliche Einordnung, allerdings eher Meinungsbeitrag).

Hinweis:

Die obigen Quellen dienten zur Erstellung dieses Whitepapers; insbesondere wurden gesetzliche Anforderungen aus offiziellen Dokumenten und Praxisempfehlungen aus Fachartikeln zusammengeführt. Alle Informationen wurden sorgfältig verifiziert, dennoch ersetzt dieses Whitepaper keine Rechtsberatung.

Wenn Sie Fragen zu diesem Whitepaper haben oder einen NIS2-Compliance-Check für Ihr Unternehmen wünschen, stehen wir Ihnen gerne zur Verfügung. Sprechen Sie uns unverbindlich an – gemeinsam finden wir heraus, wie wir Ihre Sicherheit stärken können.

Ihre Cybersicherheit ist unser Auftrag.

Vielen Dank für Ihr Interesse!

Kontakt

SpaceNet AG
Joseph-Dollinger-Bogen 14,
80807 München, Deutschland
Telefon: +49 89 32356–0
E-Mail: info@space.net
Web: www.space.net