WHITEPAPER

NIS2 und die Lieferkette



Welche Anforderungen kommen auf Zulieferer, Dienstleister und andere Akteure der Supply Chain zu?

ESET Cybersecurity
Progress. Protected.

ESET.DE/NIS2

Einleitung

In der heutigen digitalen Welt ist IT-Sicherheit ein entscheidender Faktor für Organisationen jeder Größe und Branche. Die steigende Bedeutung wird durch die Richtlinie NIS 2.0 (Network and Information Systems Directive 2.0) auf europäischer Ebene unterstrichen und weiter verstärkt.

Neben den gesetzlichen Anforderungen spielt die Risikominimierung eine zentrale Rolle für alle Organisationen, um nicht in eine bedrohliche finanzielle oder existenzielle Schieflage nach einem Cyberangriff zu geraten. Unabhängig von bevorstehenden Gesetzesänderungen müssen Unternehmen und Institutionen bereits heute angemessene Maßnahmen ergreifen, um sich vor digitalen Attacken zu schützen. Dahingehende Pflichten der Geschäftsleiter bestehen bereits heute. Der hierbei geforderte Stand der Technik ist jedoch eine oftmals als oft vage wahrgenommene Anforderung, was aus rechtlicher Sicht unzutreffend ist. Die Bestimmung der inhaltlichen Anforderungen ist im Einzelfall indes aufwändig und unterbleibt aus diesem Grund vielfach.

Es ist von großer Bedeutung, dass Organisationen die immense gesellschaftliche und geopolitische Relevanz der IT-Sicherheit verstehen und die Konsequenzen ihres Handelns oder Nichthandelns erkennen. Die bisher in den Medien erschienenen Sicherheitsvorfälle verdeutlichen den dringenden Handlungsbedarf, der den Gesetzgeber zum Eingreifen veranlasst hat. Und das ist sicherlich bloß der berüchtigte Eisberg, die Dunkelziffer der Vorfälle dürfte deutlich größer sein. Die bloße Eigenmotivation zur Schadensprävention hat sich als unzureichend erwiesen.

Allgemeine Gesetze zur ordnungsgemäßen Geschäftsorganisation und Sorgfalt haben Unternehmen nicht genug Druck gemacht, angemessene IT-Sicherheitsmaßnahmen zu ergreifen. Die bereits existierenden Anforderungen wurden oft ignoriert oder nur unzureichend umgesetzt. Die Richtlinie NIS 2.0 adressiert diesen Bedarf und bringt spezifische gesetzliche Vorgaben für die IT-Sicherheit, die für einen erheblichen Teil der Wirtschaft und zahlreiche öffentliche Stellen gelten werden.

Dieses Whitepaper widmet sich vor allem der Frage, welche Unternehmen und Organisationen voraussichtlich von den neuen gesetzlichen Vorgaben betroffen sein werden. Es ist ratsam, sofort entsprechende Maßnahmen zu ergreifen und nicht auf den Erlass des deutschen Gesetzes zu warten, das die Vorgaben der Richtlinie NIS 2.0 für Unternehmen in Deutschland verbindlich machen wird. Die Richtlinie fordert von Deutschland, diese Vorschriften bis zum 17. Oktober 2024 zu erlassen und ab dem 18. Oktober 2024 national anzuwenden.

Durch proaktive Maßnahmen und die Auswahl einer geeigneten Strategie kann eine erfolgreiche Risikominimierung zeitnah erreicht werden. Angesichts der üblicherweise langen Einführungszeiten von IT-Projekten ist es jedoch allen Unternehmen dringend zu empfehlen, entsprechende Initiativen zur Implementierung angemessener Maßnahmen umgehend zu ergreifen.

Ich hoffe, Sie erhalten beim Lesen einen informativen Einblick in das Thema.

Stefan Sander

Fachanwalt für IT-Recht
Datenschutzbeauftragter (TÜV)

SDS Rechtsanwälte Sander
Schöning PartG mbB

Autor:
Stefan Sander / SDS Rechtsanwälte
Sander Schöning PartG mbB
Rechtsanwalt - Fachanwalt für IT-Recht -
Datenschutzbeauftragter (TÜV)

Co-Autor:
Michael Klatte / ESET Deutschland GmbH
PR Manager

Auflage 1; März 2024

ESET.DE/NIS2

Inhaltsverzeichnis

1. Der Stand der Dinge bei NIS2 4

Von der Idee zur EU-Richtlinie 4
Aktuelle rechtliche Unsicherheit – Welches Gesetz gilt eigentlich und ab wann? 4
Sicherheit in der Unsicherheit 5

2. Diese Organisationen werden definitiv betroffen sein 6

Über wesentliche und wichtige Einrichtungen – oder: Die Adressaten des Gesetzes 6
Zugehörigkeit zu einem bestimmten Sektor 8
Erstes Kriterium 8
Zweites Kriterium 10
So werden wirtschaftliche Kennzahlen ermittelt 11

3. Was bedeutet das für die Unternehmen der Lieferkette? 12

Sind wir verpflichtet, nur weil wir der Lieferkette angehören? 12
Umsetzung von NIS2 erschafft neues Potential für den IT-Markt 14
Neues Marktpotenzial winkt dem Channel 14

4. Da kommt was auf Sie zu: Gesetzliche Pflichten für NIS2 15

Governance 15
Risikomanagementmaßnahmen 16
Berichtspflichten 17

5. Fazit 18

Wir unterstützen Sie bei der Umsetzung der NIS2-Richtlinie 18

Anhang: ESET Lösungen für NIS2-Compliance 19

1. **Der Stand der Dinge** bei NIS2

Von der Idee zur EU-Richtlinie

In einer Zeit, in der viele europäische Vorschriften oft kontrovers diskutiert werden, finden einige von ihnen jedoch breite Zustimmung. Während einige Regelungen der Europäischen Union – wie beispielsweise die Vorschriften zur Krümmung von Bananen oder Lautstärke von Dudelsäcken – fragwürdig erscheinen mögen, hat die EU in den Bereichen Datenschutz und Cybersicherheit Standards gesetzt. Die Datenschutz-Grundverordnung (DS-GVO) führte neue Maßstäbe für den Schutz personenbezogener Daten ein. Die jüngste Aktualisierung der „Netzwerk- und Informationssicherheit"-Richtlinie (NIS2) schickt sich an, die Fähigkeiten zur Cyberabwehr in der Fläche erheblich zu erhöhen.

Was ursprünglich mit der Idee startete, den Schutz kritischer Infrastrukturen zu verbessern, erwies sich aufgrund der rapiden, fortschreitenden Entwicklungen – insbesondere der Bedrohungslage – schnell als überarbeitungsbedürftig. Die gesetzlichen Regelungen von 2016 wurden Ende 2020 dahingehend überprüft, dass die anfänglichen Anforderungen den aktuellen Bedrohungen nicht mehr gerecht wurden. Ende 2022 wurde das Gesetzgebungsverfahren der Europäischen Union abgeschlossen, welches nicht nur konkretere und umfassendere inhaltliche Vorgaben zur IT-Sicherheit mit sich brachte, sondern auch den Geltungsbereich des Gesetzes erheblich erweiterte. Während zuvor ausschließlich Betreiber kritischer Infrastrukturen betroffen waren, verlangt die künftige Rechtslage gemäß der Richtlinie NIS 2.0 auch von mittleren Unternehmen zahlreicher Branchen, angemessene technische und organisatorische Maßnahmen (TOM) zu ergreifen – und das bis ins Detail.

Aktuelle rechtliche Unsicherheit
– Welches Gesetz gilt eigentlich und ab wann?

Die Richtlinie (EU) 2022/2555 („**NIS2**") ist ein von der Europäischen Union verabschiedetes Gesetz. Es trat am 17. Januar 2023 in Kraft, jedoch begründet es nicht unmittelbar die besagten gesetzlichen Pflichten für Unternehmen in Deutschland. Hätte die EU dieses Gesetz als Verordnung und nicht als Richtlinie erlassen, wäre es direkt und zwingend in allen Mitgliedsstaaten der EU anwendbar, und die dort ansässigen Unternehmen wären direkt betroffen. Es hätte sogar Vorrang vor etwaigen nationalen Gesetzen der Mitgliedsstaaten, falls diese andere inhaltliche Aussagen enthielten. Jedoch ist es keine Verordnung, sondern eine Richtlinie geworden.

Konkrete gesetzliche Vorgaben zur IT-Sicherheit, die in manchen Details durchaus anspruchsvoll umzusetzen sein werden (wie etwa die Erfüllung von Berichtspflichten bei erheblichen Sicherheitsvorfällen innerhalb von 24 Stunden mit erheblicher Detailtiefe), verdienen bereits im Vorfeld ihres Inkrafttretens Aufmerksamkeit. Welche spezifischen gesetzlichen Vorgaben jedoch aufgrund der NIS2-Richtlinie in Deutschland erlassen werden und welche Unternehmen letztendlich konkret verpflichtet sein werden, ist zum jetzigen Zeitpunkt nicht abschließend abzuschätzen.

Denn ein derartiges **deutsches Gesetz** ist noch nicht vom Gesetzgeber verabschiedet.

Sicherheit in der Unsicherheit

Als Gesetz der EU richtet sich die NIS2-Richtlinie wie alle Richtlinien der EU ausschließlich an die Mitgliedsstaaten der EU, was bedeutet, dass es den deutschen Staat insgesamt betrifft. Deutschland ist verpflichtet, seine Gesetze so anzupassen, dass sie mit den Inhalten der NIS2-Richtlinie übereinstimmen. Offiziell trägt das Gesetz den Titel „Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union". Die Bezeichnung „NIS2" ergibt sich lediglich aus dem Zusammenhang, da NIS2 die ältere Richtlinie (EU) 2016/1148 aufhebt und durch inhaltlich überarbeitete, strengere Regelungen ersetzt. Die Richtlinie von 2016 wiederum trug den Titel „Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union" (NIS-Richtlinie).

Die Verpflichtung Deutschlands zur Umsetzung der Richtlinie in nationales Recht wurde mit dem Inkrafttreten der NIS2-Richtlinie am 17. Januar 2023 begründet, wofür bestimmte Fristen festgelegt wurden. Bis zum 17. Oktober 2024 müssen alle EU-Mitgliedstaaten die erforderlichen Vorschriften erlassen und veröffentlichen, um den Anforderungen der Richtlinie zu entsprechen. Gemäß der Richtlinie müssen die Mitgliedsstaaten diese Vorschriften ab dem **18. Oktober 2024** anwenden.

Die derzeitige rechtliche Unsicherheit besteht darin, dass die NIS2-Richtlinie den Mitgliedstaaten nicht verbietet, strengere Bestimmungen zu erlassen oder beizubehalten, die ein höheres Niveau der Cybersicherheit gewährleisten, solange diese Bestimmungen mit den Verpflichtungen der Mitgliedstaaten gemäß dem Unionsrecht, insbesondere der NIS2 Richtlinie, im Einklang stehen. Deutschland hat also die Möglichkeit, im eigenen Gesetz strengere Anforderungen festzulegen und/oder den Kreis derjenigen, die von den gesetzlichen Pflichten erfasst werden, zu erweitern.

Im Umkehrschluss ergibt sich aus Artikel 5 der NIS2-Richtlinie zur **Mindestharmonisierung** in der EU, dass Unternehmen in Deutschland sich bereits darauf vorbereiten können, zumindest mit den Inhalten der Richtlinie konfrontiert zu werden. Mindestens diejenigen Unternehmen, die gemäß den Vorgaben der Richtlinie von den nationalen Gesetzen adressiert werden müssen, werden den entsprechenden Verpflichtungen unterliegen. Für diesen Kreis der sog. „Normadressaten" steht bereits fest, dass sie ab dem Zeitpunkt der Verpflichtung zur Anwendung der Vorschriften die inhaltlichen Pflichten erfüllen müssen, die zumindest minimal vorgesehen sind.

Wenn also im Zusammenhang mit NIS2 oder dem deutschen Umsetzungsgesetz (welches noch nicht existiert) von den zukünftigen Normadressaten heute die Frage gestellt wird, welchen Übergangszeitraum das deutsche Gesetz haben wird – innerhalb dessen sich diese Unternehmen intern anpassen können und die besagten IT-Einführungsprojekte beginnen und erfolgreich abschließen können – ist gemäß Artikel 41 Absatz 1 Satz 2 der NIS2-Richtlinie zu antworten:

Der **Übergangszeitraum** ist die Zeit, die jetzt verstreicht und **am 18. Oktober 2024 endet**.

2. Diese Organisationen
werden definitiv betroffen sein

Über wesentliche und wichtige Einrichtungen – oder: Die Adressaten des Gesetzes

Die zukünftige deutsche Rechtslage wird zumindest die Unternehmen verpflichten, die den Kriterien entsprechen, die die NIS2-Richtlinie in ihren Artikeln 2 und 3 zwingend vorschreibt. Dabei spricht die Richtlinie von „wesentlichen und wichtigen Einrichtungen", in Deutschland werden jedoch Entwürfe für ein Umsetzungsgesetz diskutiert, die diese beiden Kategorien als "besonders wichtige Einrichtungen und wichtige Einrichtungen" bezeichnen. Der aktuell bekannte Entwurfsstand ist der Referentenentwurf des Bundesministeriums des Innern und für Heimat (BMI) vom 22.12.2023. Über diesen Entwurf besteht aber schon allein innerhalb der Bundesregierung, also zwischen Ressorts, noch keine Einigkeit – geschweige denn es hätte eine politische Diskussion über diesen im Bundestag auch nur begonnen, welche auch noch zu führen sein wird.

Einen ersten, kurzen Überblick gibt die folgende Abbildung. Der Kreis der Normadressaten, also der betroffenen „Einrichtungen", wird durch eine Tätigkeit in einem bestimmten Sektor sowie durch zwei spezifische Eigenschaften konkretisiert, von denen beide erfüllt sein müssen. Auf diese beiden Eigenschaften, wirtschaftliche Kennzahlen sowie die Größe des Unternehmens, gehen wir in diesem Kapitel später detailliert ein.

Die aktuelle rechtliche Situation in Deutschland, die noch durch die mittlerweile aufgehobene ältere Richtlinie (EU) 2016/1148 (NIS-Richtlinie) geprägt ist, unterscheidet sich von der zukünftigen Rechtslage. Die erwartete Gesetzesänderung betrifft den auf europäischer Ebene geänderten Anknüpfungspunkt. Aktuell richten sich die gesetzlichen Anforderungen an Betreiber kritischer Infrastrukturen. Ob eine Infrastruktur „kritisch" ist, wird anhand von Schwellenwerten bestimmt, die den Versorgungsgrad für die Bevölkerung berücksichtigen und sich auf eine Referenzgruppe von 500.000 Bürgern beziehen. Die fragmentierten Schwellenwert-Tabellen für verschiedene Arten von Anlagen werden in Bezug auf die spezifische Rechtslage für die IT-Sicherheit durch einheitliche Regeln ersetzt. Zukünftig werden die gesetzlichen Verpflichtungen zur IT-Sicherheit nicht mehr davon abhängig sein, ob eine von einer Einrichtung betriebene Anlage für die Versorgungssicherheit der Bevölkerung als kritisch eingestuft wird. Stattdessen werden ganze Einrichtungen anhand wirtschaftlicher Kennzahlen und der Größe der Einrichtung zu den Adressaten der Verpflichtungen.

Die Regelungen für kritische Infrastrukturen bleiben übrigens erhalten. Diese werden auch weiterhin als Einrichtungen oder Betreiber von Anlagen oder Teilen davon definiert, die hinsichtlich ihres Versorgungsgrads für die Bevölkerung als „kritisch" eingestuft werden. Diese Regelungen betreffen die physische Sicherheit kritischer Infrastrukturen und die entsprechenden Pflichten der Betreiber.

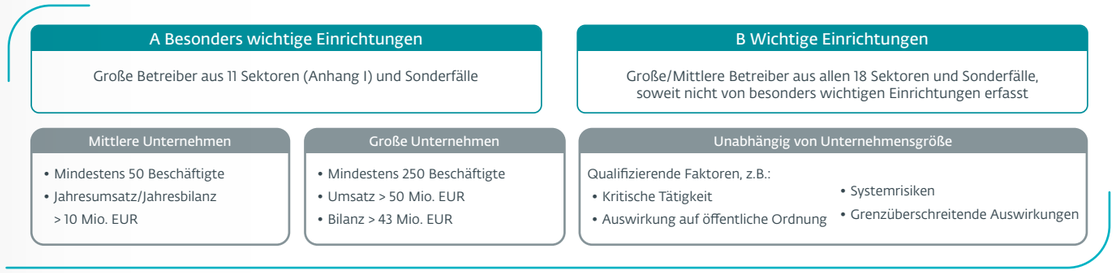


Abb. 1: Schwellenwerte und Definitionen nach NIS-2-Richtlinie

Erstes Kriterium

Zugehörigkeit zu einem bestimmten Sektor

Gemäß der NIS2-Richtlinie werden als „wesentliche" Einrichtungen (in Deutschland demnächst wohl „besonders wichtige Einrichtungen") die Einrichtungen der in Anhang I der Richtlinie aufgeführten Art betrachtet, die auch das zweite Kriterium erfüllen (siehe unten). Darüber hinaus gibt es in Artikel 3 der NIS2-Richtlinie einige Sonderfälle die, ohne weitere Kriterien zu erfüllen, auch zu dieser Kategorie von Einrichtungen gehören, darunter die Betreiber kritischer Infrastrukturen. Diese werden, als Teilmenge der „wesentlichen" bzw. „besonders wichtigen" Einrichtungen, in gleichem Umfang wie die anderen Einrichtungen dieser Kategorie mit Pflichten zur IT-Sicherheit belegt.

Als (nur) „wichtige" Einrichtungen betrachtet die NIS2-Richtlinie (in Deutschland künftig wohl „wichtige Einrichtungen") die Einrichtungen der in Anhang I oder II der Richtlinie aufgeführten Art, die auch das zweite Kriterium erfüllen (siehe unten) und die nicht bereits als „wesentliche" Einrichtungen im Sinne der Richtlinie gelten.

Sektoren nach Anhang I	Sektoren nach Anhang II
Energie	Post- und Kurierdienste
Verkehr und Transport	Abfallwirtschaft
Bankwesen	Produktion, Herstellung und Handel mit chemischen Stoffen
Finanzmärkte	Produktion, Verarbeitung und Handel von Lebensmitteln
Gesundheitswesen	Verarbeitendes Gewerbe/Herstellung von Waren
Trinkwasser	Anbieter digitaler Dienste
Abwasser	Forschungseinrichtungen
Digitale Infrastruktur	
ICT* Service Management (Managed Service Provider - MSP)	
Öffentliche Verwaltung	
Weltraum	

Abb. 2: Sektorenübersicht nach NIS2-Richtlinie

* Information and Communication Technology

In beiden Anhängen der NIS2-Richtlinie wird die Zugehörigkeit einer Einrichtung zu einem der Sektoren noch etwas weiter präzisiert (in vorstehender Abbildung ausgelassen), was hier anhand zweier Beispiele betrachtet werden soll. IT-Dienstleister und Zulieferer werden es geahnt haben: Sie erfüllen allein durch ihre Branchenzugehörigkeit schon einmal eine der Anforderungen der NIS2-Richtlinie. Sektor **Nr. 9 aus Anhang I**, welcher in der deutschen Sprachfassung mit „Verwaltung von IKT-Diensten (Business-to-Business)" bezeichnet wird, gliedert sich auf in die Anbieter verwalteter Dienste und die Anbieter verwalteter Sicherheitsdienste. Diese beiden Begriffe haben für Zwecke der NIS2-Richtlinie jeweils eine feststehende Bedeutung. Hier werden gezielt Managed Service Provider (MSP) angesprochen.

Gemäß Artikel 6 Nummer 39 der NIS2-Richtlinie wird ein **„Anbieter verwalteter Dienste"** als eine Einrichtung definiert, die Dienste im Zusammenhang mit der Installation, der Verwaltung, dem Betrieb oder der Wartung von IKT-Produkten, Netzen, Infrastruktur, Anwendungen oder jeglicher anderer Netz- und Informationssysteme durch Unterstützung oder aktive Verwaltung erbringt, sei es in den Räumlichkeiten der Kunden oder aus der Ferne.

Gemäß Artikel 6 Nummer 40 der NIS2-Richtlinie wird ein **„Anbieter verwalteter Sicherheitsdienste"** als ein Anbieter verwalteter Dienste (siehe oben, d. h. die Sprache ist von einer Teilmenge) definiert, der Unterstützung für Tätigkeiten im Zusammenhang mit dem Risikomanagement im Bereich der Cybersicherheit durchführt oder erbringt. Beispiele hierfür sind Dienstleister, die Services wie Managed Detection and Response (MDR) anbieten oder allgemeine Managed Security Services Provider (MSSP) sind.

Selbstverständlich gibt es auch andere Bereiche, die nicht in erster Linie mit IT in Zusammenhang stehen. Ein Beispiel wäre die Automobilindustrie, die einen Teil des Sektors mit der Nr. 5 in Anhang II ausmacht. In der deutschen Sprachfassung ist der Sektor betitelt mit „Verarbeitendes Gewerbe/Herstellung von Waren" und gliedert sich in sechs Bereiche auf. Einer davon ist die Herstellung von Kraftwagen und Kraftwagenteilen, d.h. gemeint ist der Wirtschaftszweig, in den Automobilhersteller und deren Zulieferer fallen. Die Lieferkette ist also nicht „als solche" vom Gesetzgeber adressiert, sondern die Betroffenheit der Unternehmen aus der Lieferkette ergibt sich über ihre eigene Zugehörigkeit zu einem bestimmten „Wirtschaftszweig". Darüber hinaus kommt „die Lieferkette" nochmals ins Spiel, bei den konkret zu ergreifenden Maßnahmen, worauf weiter unten eingegangen wird.

Zweites Kriterium

Wirtschaftliche Kennzahlen der Einrichtung („size cap")

Neben der Zugehörigkeit zu einem der Sektoren enthält die NIS2-Richtlinie als zweites Kriterium klare Vorgaben, ab wann ein Unternehmen unter die Richtlinie fällt. Politisch gewollt war es, dass bereits **„mittlere Unternehmen"** von den **Verpflichtungen** erfasst sein sollen.

Es stellt sich die Frage, wer oder was als „mittleres Unternehmen" oder als „großes Unternehmen" überhaupt bezeichnet wird. Die Antwort darauf gibt der im Laufe der Jahre immer wieder überarbeitete Benutzerleitfaden zur **Definition von KMU** der Europäischen Kommission, Generaldirektion Binnenmarkt, Industrie, Unternehmertum und KMU[1]. Diese Definition wird von der NIS2 Richtlinie ausdrücklich in Bezug genommen und ist damit für Deutschland bei Umsetzung der Richtlinie in nationales Recht eine zwingende Vorgabe. Die Anzahl der Mitarbeiter und eine wirtschaftliche Kennzahl, der Jahresumsatz oder die Jahresbilanzsumme entscheiden darüber, ob das Unternehmen NIS2 befolgen muss oder nicht. Konkret formulierte der europäische Gesetzgeber: Die NIS2-Richtlinie gilt für öffentliche oder private Einrichtungen der in den Anhang I oder II der Richtlinie genannten Art, die nach Artikel 2 des Anhangs der Empfehlung 2003/361/EG (dies ist die europäische KMU-Definition) als mittlere Unternehmen gelten oder die Schwellenwerte für mittlere Unternehmen überschreiten und ihre Dienste in der Union erbringen oder ihre Tätigkeiten dort ausüben. Artikel 3 Absatz 4 des Anhangs dieser Empfehlung gilt nicht für die Zwecke der NIS2-Richtlinie.

Die Betrachtung von Sonderfällen bleibt im Rahmen dieses Whitepapers außen vor. Ist das Unternehmen **mindestens** als **„mittleres Unternehmen"** im Sinne der europäischen KMU-Definition anzusehen oder etwaig größer, ist damit das zweite Kriterium für die Einordnung als „wichtige Einrichtung" erfüllt. Für die – vorrangige – Einordnung als „wesentliche Einrichtung" im Sinne der Richtlinie (in Deutschland demnächst wohl „besonders wichtige Einrichtungen") muss das Unternehmen **größer als** ein **mittleres Unternehmen** im Sinne der europäischen KMU-Definition sein, wobei anzumerken ist, dass dort für solche Unternehmen kein Begriff definiert ist.

Zahlreiche Mittelständler, nicht nur in Deutschland, dürften insbesondere von den Schwellenwerten für die Betriebsgröße von mittleren Unternehmen überrascht sein. Der Bereich der mittleren Unternehmen beginnt bei 50 Mitarbeitern und endet bei 249 Mitarbeitern, wobei der Begriff Mitarbeiter in diesem Kontext eigenständig definiert wird. Das Kriterium umfasst nicht nur Voll- und Teilzeitkräfte, sondern auch Zeitarbeiter sowie Saisonpersonal. Es schließt sogar mitarbeitende Eigentümer sowie Teilhaber ein, die eine regelmäßige Tätigkeit in dem Unternehmen ausüben und finanzielle Vorteile aus dem Unternehmen ziehen.

1 https://www.bafa.de/SharedDocs/Downloads/DE/kmu_handbuch_eu.html

So werden wirtschaftliche Kennzahlen ermittelt

Die europäische KMU-Definition gibt nicht nur die wirtschaftlichen Kennzahlen vor (Anzahl der Mitarbeiter, Jahresumsatz bzw. Jahresbilanzsumme), die zur Beschreibung von KMU dienen, sondern legt darüber hinaus fest, woher diese Zahlen kommen bzw. welche Zahlen zugrunde zu legen sind.

Zur Bestimmung der Einstufung gemäß der KMU-Definition sind **Konsolidierungen** erforderlich, bei denen wirtschaftliche Kennzahlen von sog. „verbundenen Unternehmen" und von sog. „Partnerunternehmen" zusammengefasst werden. Ein Unternehmen wird als eigenständig betrachtet, wenn es weder Beteiligungen an anderen Unternehmen hält noch andere Unternehmen an ihm beteiligt sind. Bei eigenständigen Unternehmen kommt es nur auf die eigenen wirtschaftlichen Kennzahlen an. Die Durchführung der Konsolidierung, einschließlich der Gewichtung, wird im Benutzerleitfaden zur Definition von KMU der Europäischen Kommission, Generaldirektion Binnenmarkt, Industrie, Unternehmertum und KMU ausführlich erläutert (zur Fundstelle, siehe oben). Dort wird nicht nur der vollständige Text der europäischen KMU-Definition bereitgestellt (Anmerkung: Artikel 3 Absatz 4 des Anhangs der Empfehlung gilt nicht für die Zwecke der NIS2-Richtlinie), sondern es werden auch zahlreiche Beispiele zur Veranschaulichung der Konsolidierung erläutert.

3. Was bedeutet das
für die Unternehmen der Lieferkette?

Mit der NIS2-Richtlinie und der nationalen Gesetzgebung kommen auf die Lieferkette eine besondere Verantwortung zu. IT-Dienstleister, die als MSP agieren, fallen unter den Sektor 9 des Anhangs I zur NIS2-Richtlinie und kommen daher als „besonders wichtige Einrichtungen" in Betracht. Gerade im Hinblick auf jüngste Sicherheitsvorfälle ist diese Einstufung nicht überraschend. Im Oktober 2023 legte eine Cyberattacke die Verwaltungen und Rathäuser in mehr als 70 Kommunen in NRW lahm. Ziel des Angriffs war das Netzwerk des IT-Dienstleisters Südwestfalen-IT.

Sind wir verpflichtet, nur weil wir der Lieferkette angehören?

Die NIS2-Richtlinie hat keinen dedizierten Anknüpfungspunkt für „Mitglieder einer Lieferkette", soweit es um die Frage geht, welches Unternehmen von den Rechtspflichten zur IT-Sicherheit betroffen werden wird. Jedoch werden durch die umschriebenen Kriterien zahlreiche Unternehmen der Supply Chain erfasst. Was könnte es also für die Lieferkette konkret bedeuten, wenn ein Unternehmen nach allgemeinen, oben beschriebenen Kriterien vom Gesetz adressiert wird?

Die zukünftige deutsche Gesetzeslage wird Unternehmen dazu verpflichten, sich in besonderem Maße gegen Gefahren aus der Lieferkette und die anderen Unternehmen der Lieferkette zu schützen. Es sind Regelungen zu erwarten, die zur Umsetzung angemessener technischer und organisatorischer Maßnahmen (TOM) verpflichten und diese Pflichten für die Gefahrenquelle Lieferkette präzisieren (derartiges wird es nach Maßgabe der NIS2-Richtline geben, dazu weiter unten).

Dass der bloße Umstand, Teil der Lieferkette zu sein, dazu führen kann, allein deswegen zum Kreis derjenigen zu gehören, an den die gesetzlichen Vorgaben zur IT-Sicherheit adressiert sind, ist nicht abwegig. Denn dies ist gegenwärtig der Fall, d.h. die Rechtslage in Deutschland, die derzeit noch gilt, kennt gesetzliche Pflichten zur IT-Sicherheit speziell in Bezug auf Unternehmen, die der Lieferkette angehören. Unternehmen fallen dann in den Anwendungsbereich, wenn sie als Zulieferer wegen ihrer Alleinstellungsmerkmale von wesentlicher Bedeutung für ein anderes Unternehmen sind, sofern dieses andere Unternehmen als ein Unternehmen in besonderem öffentlichen Interesse angesehen wird. Die zukünftige deutsche Gesetzeslage zur IT-Sicherheit nach Maßgabe der NIS2-Richtlinie wird einen solchen Anknüpfungspunkt jedoch aller Voraussicht nach nicht mehr kennen. Denn es gibt keine Sondervorschriften im Regelungskonzept der NIS2-Richtlinie, die Unternehmen allein deshalb zu Normadressaten machen, weil sie Teil der Lieferkette sind, falls jenes Unternehmen, welches beliefert wird, für sich genommen in den Anwendungsbereich fällt. Ein solcher „abgeleiteter" Grund zur Verpflichtung ist nicht vorgesehen. Vielmehr ging der EU-Gesetzgeber davon aus, dass über das zweite Kriterium („size cap") die Anforderungen so niedrig angesetzt wurden, dass alle aus Sicht des Gesetzgebers „relevanten" bzw. aus seiner Sicht regelungsbedürftigen Unternehmen vom Anwendungsbereich der NIS2-Richtlinie erfasst werden. Es gab damit schlicht keinen Bedarf, über einen zusätzlichen Anknüpfungspunkt Supply Chain weitere Unternehmen in den Anwendungsbereich einzubeziehen, ergänzend zu den ohnehin erfassten Unternehmen. Ebenfalls ist jedoch festzustellen, dass es auch keine Ausnahmen für Zulieferer gibt, Unternehmen also etwaig aus dem Kreis der Normadressaten ausgenommen würden, weil sie „nur" Zulieferer sind. Dass der deutsche Gesetzgeber insoweit „konzeptionell" über die Mindestharmonisierung in der EU hinausgehen wird, ist zwar möglich, derzeit aber nicht abzusehen.

Hinsichtlich der Lieferkette im Bereich IT ist festzustellen, dass über die in den Anhängen der NIS2-Richtlinie enthaltenen Formulierung wohl alle Unternehmen „der Lieferkette" erfasst werden sollten. Dies betrifft insbesondere den Bereich, in dem Unternehmen der Supply Chain nicht bloß Vorlieferanten sind, die einen Gegenstand wie z.B. ein halbfertiges Erzeugnis oder eine Maschine verkaufen, sondern die während des Betriebs der IT ihre Leistungen erbringen bzw. gerade der ausgelagerte Betrieb der IT die Leistungserbringung dieser Unternehmen ist (siehe oben, Sektor Nr. 9 aus Anhang I (MSP)).

Auch hinsichtlich der Lieferkette anderer Branchen ist festzustellen, dass nicht nur die (großen) Hersteller (der Endprodukte, wie oben im Beispiel „Kraftwagen") erfasst werden, sondern über den Begriff der Wirtschaftstätigkeit im Sinne der Statistischen Systematik der Wirtschaftszweige regelmäßig auch die Zulieferer der „Big Player" des jeweiligen Sektors miterfasst werden.

Umsetzung von NIS2 erschafft neues Potential für den IT-Markt

Die technische Umsetzung der NIS2-Richtlinie, die Registrierungs- und Meldepflichten und die Einhaltung der weiteren grundsätzlichen Rahmenbedingungen werden viel Geld verschlingen. Allein für Deutschland gehen Experten von einem jährlichen Erfüllungsaufwand von mehr als 1,65 Milliarden Euro aus. Was für die betroffenen Organisationen Kosten sind, könnte man auf der anderen Seite auch als Chance sehen: Hier entsteht ein zusätzliches Marktpotential für Security-Hersteller, IT-Dienstleistungsunternehmen und die Digitalwirtschaft generell. Viele Unternehmen und Institutionen werden sicherheitstechnisch deutlich aufrüsten müssen.

Doch nicht jeder hat die notwendigen personellen Ressourcen parat, um diese Aufgabe aus eigener Kraft stemmen zu können. Ihnen bleibt fast nichts anderes übrig, als auf externe Unterstützung zurückzugreifen. Es entsteht deshalb ein zusätzliches Marktpotential für die Beratungsbranche, für IT-Sicherheitsbeauftragte, für ISMS-Spezialisten und -Auditoren, für Systemintegratoren und nicht zuletzt für Dienstleister, die mit „as-a-Service–Angeboten" auf dem Markt sind.

Dies ist definitiv auch und gerade für IT-Dienstleister ein interessantes Geschäftsfeld. Die Grundidee der NIS2-Richtlinie, erhöhte Cyber-Resilienz der Volkswirtschaft insgesamt, endet nicht an Grenzen. Deshalb sollten Organisationen ihr eigenes Schutzniveau hinterfragen und die Vorschläge zur digitalen Widerstandskraft gründlich durchdenken. So mancher Firmenlenker wird analysieren, dass die eingesetzten Security-Maßnahmen nicht mehr zur (weltweiten) Gefahrenlage passen.

Neues Marktpotenzial winkt dem Channel

Den IT-Dienstleistern, die in der Regel als Trusted Advisor für ihre Kunden fungieren, kommt hier eine besondere Rolle und Verpflichtung zu. Es gilt, Kunden eindringlich auf Defizite hinzuweisen und gemeinsam mit ihnen individuelle und angemessene Lösungen zu entwickeln. Hierbei wird es künftig stärker als in der Vergangenheit nötig sein, über arbeitsteilige Konzepte nachzudenken. Damit ist gemeint, dass ein Unternehmen mit seinen eigenen IT-Ressourcen nur Teile der IT-Sicherheitslösung betreut und darüber hinaus auf kompetente Dienstleister zurückgegriffen wird. Dies können beispielsweise Services wie Endpoint Detection and Response (EDR), Threat Intelligence oder andere professionelle IT-Security Services sein, die sich in ein sinnvolles Gesamtlösungskonzept integrieren lassen. Für den Channel lohnt es sich darüber nachzudenken, mit welchen potenziellen Partnern und Allianzen man sich aufstellen möchte, um das entstehende Marktpotential erschließen und den Kunden angepasste Lösungen und ein angemessenes Schutzniveau bieten zu können.

4. Da kommt was auf Sie zu: Gesetzliche Pflichten für NIS2

Der Gesetzgeber der NIS2-Richtlinie betrachtet IT-Sicherheit als „Chefsache", was sich in der Umsetzung der Richtlinie demnächst expressis verbis auch im deutschen Gesetz wiederfinden wird. Zudem hat er die zu ergreifenden Maßnahmen der IT-Sicherheit deutlich differenzierter als bislang geregelt und dabei auch „die Lieferkette" in den Blick genommen.



Governance

Die Leitungsorgane wesentlicher und wichtiger Einrichtungen werden zukünftig gesetzlich verpflichtet werden, die von diesen Einrichtungen ergriffenen **Risikomanagementmaßnahmen** im Bereich der Cybersicherheit **zu billigen** und **ihre Umsetzung zu überwachen**. Bei Verstößen gegen die Vorgaben zu Risikomanagementmaßnahmen können die Leitungsorgane **persönlich verantwortlich** gemacht werden.

Darüber hinaus werden die Mitglieder der Leitungsorgane an Schulungen teilnehmen müssen – und zwar ausdrücklich per Gesetz. Ziel ist es, dass sie ausreichende Kenntnisse und Fähigkeiten erwerben, um überhaupt die Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste einschätzen und beurteilen zu können.

Risikomanagementmaßnahmen

Wesentliche und wichtige Einrichtungen werden gesetzlich verpflichtet werden, geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen zu ergreifen. Dabei sollen diese Organisationen die Maßnahmen beherrschen und die Auswirkungen von Sicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Bereiche verhindern oder zumindest möglichst gering halten. Wie oben bereits angedeutet, werden die zukünftigen gesetzlichen Vorgaben demnach ausdrücklich (auch) auf die **Gefahrenquelle „Lieferkette"** bezogen sein – **und**, andersherum betrachtet, auch den **Schutz der Lieferkette** verlangen.

Die zu ergreifenden Maßnahmen müssen unter Berücksichtigung des Stands der Technik und gegebenenfalls der einschlägigen europäischen und internationalen Normen sowie unter Berücksichtigung der Kosten der Umsetzung ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist. Die Auswahl der Maßnahmen muss auf einem gefahrenübergreifenden Ansatz beruhen, der darauf abzielt, sowohl die Netz- und Informationssysteme als auch die physische Umwelt dieser Systeme vor Sicherheitsvorfällen und deren Folgen zu schützen.

Letztlich müssen die Maßnahmen zumindest Folgendes umfassen:

a) Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme;

b) Bewältigung von Sicherheitsvorfällen;

c) Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement;

d) Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Dienstean-bietern;

e) Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen;

f) Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit;

g) grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit;

h) Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung;

i) Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen;

j) Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

Berichtspflichten

Wesentliche und wichtige Einrichtungen sind verpflichtet, ihr entsprechendes CSIRT (Computer-Notfallteam) oder gegebenenfalls eine zuständige Behörde unverzüglich über jeden erheblichen Sicherheitsvorfall zu informieren. Unter bestimmten Umständen müssen diese Einrichtungen auch die Empfänger ihrer Dienste, **also die Lieferkette** zumindest nach unten hin, unverzüglich über solche erheblichen Sicherheitsvorfälle benachrichtigen, die die Erbringung des jeweiligen Dienstes beeinträchtigen könnten.

Besonders wichtig ist zu betonen, dass gemäß der NIS2-Richtlinie nach der Frühwarnung (spätestens innerhalb von 24 Stunden) und der Meldung des Sicherheitsvorfalls (spätestens innerhalb von 72 Stunden) eine gesetzliche Verpflichtung zur Erstattung eines Abschlussberichts vorgesehen sein wird. Die NIS2-Richtlinie legt bereits die Mindestinhalte des Abschlussberichts fest, die unter anderem eine detaillierte Beschreibung des Sicherheitsvorfalls, einschließlich seiner Schwere und Auswirkungen, sowie Angaben zur Art der Bedrohung oder der zugrunde liegenden Ursache, die wahrscheinlich den Sicherheitsvorfall ausgelöst hat, umfassen. Bereits für die Meldung des Sicherheitsvorfalls wird eine „erste Bewertung" des Sicherheitsvorfalls sowie gegebenenfalls die Angabe sog. „indicators of compromise" (IOC) verlangt. Typische IOC sind Prüfsummen von Malware-Dateien, Virensignaturen, URLs, IP-Adressen und Domain Name System Records, z. B. von beteiligten Command-and-Control-Servern eines Botnetzes.

Um den Berichtspflichten im Falle eines erheblichen Sicherheitsvorfalls nachkommen zu können, müssen alle wesentlichen und wichtigen Einrichtungen demnach solche Technologien beschaffen und einsetzen, die sie – rein faktisch betrachtet – in die Lage versetzen, die Pflichten erfüllen zu können. Eine entsprechende Vorbereitung ist unerlässlich und umfasst neben den technischen, operativen und organisatorischen Maßnahmen, die Teil der Risikomanagementmaßnahmen sind, auch die Bereitstellung geeigneter Ressourcen bzw. Verwendung geeigneter Technologien. Nur durch eine solche Vorbereitung können die Berichtspflichten im Ernstfall erfüllt werden.

5. Fazit

Die NIS2-Richtlinie zielt darauf ab, die Cybersicherheit in der EU zu stärken, indem sie klare Anforderungen an Unternehmen stellt und die Zusammenarbeit zwischen den Akteuren in der Lieferkette fördert. Die Sicherheit der Supply Chain ist entscheidend, um Cyberangriffe auf kritische Infrastrukturen zu verhindern und die Resilienz des gesamten Systems zu gewährleisten.

Unternehmen, die unter die NIS2-Richtlinie fallen, können Zulieferer und Dienstleister dazu verpflichten, spezifische Sicherheitsmaßnahmen zu ergreifen, um ihre Systeme und Daten zu schützen. Dies bedeutet, dass Unternehmen, die als digitale Diensteanbieter eingestuft sind, ihre Lieferanten und Partner dazu auffordern können, bestimmte Sicherheitsstandards einzuhalten. Beispielsweise kann ein Energieversorgungsunternehmen, das unter die NIS2-Richtlinie fällt, von seinen Lieferanten verlangen, Schutzmaßnahmen gegen Cyberangriffe zu implementieren, um die Integrität und Verfügbarkeit seiner Dienste sicherzustellen. Es ist vor diesem Hintergrund wichtig, dass Unternehmen ihre Lieferanten und Partner aktiv in ihre Sicherheitsstrategien einbeziehen, um die digitale Resilienz zu erhöhen.

Wir unterstützen Sie bei der Umsetzung der NIS2-Richtlinie

Als europäischer Anbieter im Bereich digitaler Sicherheitslösungen helfen wir Ihnen bei der Implementierung und Erfüllung der NIS2-Vorgaben.

Dafür bieten wir verschiedene Lösungen und Möglichkeiten:

- Wissensaustausch über unsere Kanäle wie den Digital Security Guide oder unseren Corporate Blog
- Interaktive Veranstaltungen wie Workshops
- Unterstützung bei der Einhaltung und Umsetzung von NIS2-Maßnahmen
- Bereitstellung von Sicherheitslösungen, die zur Einhaltung von Vorschriften beitragen
- Unsere Spezialisten stehen Ihnen jederzeit zur Verfügung, um Ihre Fragen zu beantworten

Vereinbaren Sie einen Termin mit unseren ESET Experten



Maik Wetzel

Strategischer Experte
Strategic Business Development Director,
ESET Deutschland GmbH

ESET.DE/NIS2KONTAKT



Michael Schröder

Technischer Experte
Manager of Security Business Strategy
ESET Deutschland GmbH

MADE IN EU

ESET Lösungen für NIS2-Compliance

Bitte beachten Sie, dass unsere Inhalte keine rechtliche Beratung ersetzen. Bitte wenden Sie sich für Ihren konkreten Fall an eine Rechtsanwältin oder einen Rechtsanwalt Ihres Vertrauens.

Übrigens: Das BSIG beinhaltet für die unter das Gesetz fallenden privaten und öffentlichen Einrichtungen **umfangreiche Berichtspflichten**. Dazu gehört, dass Einrichtungen laut § 32 Abs. 1 BSIG einen erheblichen Sicherheitsvorfall **innerhalb von 24 Stunden** der zuständigen Behörde melden müssen. **Innerhalb von 72 Stunden** sollen zudem **Kompromittierungsindikatoren** (IoCs) benannt werden und **nach einem Monat soll ein umfassender Abschlussbericht** vorgelegt werden. Bei der Bereitstellung solch umfangreicher Dokumentationen können Extended Detection & Response (XDR) Lösungen wie ESET Inspect unterstützen.

In Deutschland wurde mit dem NIS-2-Umsetzungsgesetz, das im Dezember 2025 in Kraft trat, unter anderem das BSI-Gesetz (BSIG) grundlegend überarbeitet und erweitert. Von besonderer Bedeutung für viele Unternehmen sind die neu hinzugekommenen Paragraphen zu Risikomanagement (§ 30) und Meldepflichten (§ 32), die nun für deutlich mehr Sektoren und Einrichtungen gelten (siehe § 28). Die folgende Übersicht zeigt unseren Ansatz für eine mögliche Umsetzung der geforderten IT-Sicherheitsmaßnahmen unter Einsatz von ESET Lösungen.

In Österreich wurde das NIS-2-Umsetzungsgesetz im Dezember 2025 veröffentlicht und tritt im Oktober 2026 in Kraft. Weitere Informationen finden Sie ↗hier.

ESET.DE/NIS2

§ 30 Abs. 2 BSIG:

Maßnahmen nach Absatz 1 sollen den Stand der Technik einhalten, die einschlägigen europäischen und internationalen Normen berücksichtigen und müssen auf einem gefahrenübergreifenden Ansatz beruhen. Die Maßnahmen müssen zumindest Folgendes umfassen:

BSIG im Wortlaut	Unser Ansatz für eine mögliche Umsetzung	ESET Lösung	ESET PROTECT Bundles			
			MDR Ultimate	MDR	Elite	Complete
1. Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik,	Wir von ESET bzw. unsere Vertriebspartner unterstützen Sie bei der technischen Bewertung, Erstellung und Umsetzung von passenden IT-Sicherheitskonzepten entsprechend Ihrer Kundenumgebung.		Unter Umständen Bestandteil der Presales-Phase			
	Mit unserer Management-Konsole haben Sie dank Hard- und Software-Inventarisierung Ihre schützenswerten Assets im Blick und verfügen damit über eine zuverlässige Grundlage für die Risikoanalyse sowie die Erstellung Ihres Sicherheitskonzepts.	ESET PROTECT	✓	✓	✓	✓
2. Bewältigung von Sicherheitsvorfällen,	Unser Extended Detection & Response Tool ermöglicht eine umfassende Gefahrensuche und -abwehr. Ereignisse im Netzwerk werden protokolliert und zu Vorfällen zusammengefasst, sodass Sie einen Überblick darüber haben, was in Ihrer IT-Umgebung vor sich geht. So können Sie bei einem Sicherheitsvorfall schnell reagieren. Dank festgelegter Reaktionsmaßnahmen wird das Sicherheitsniveau zudem weiter gesteigert.	ESET Inspect (in Kombination mit ESET PROTECT)	✓	✓	✓	
	ESET Experten übernehmen den operativen Betrieb Ihrer ESET Inspect Instanz und damit die Überprüfung, Auswertung und Interpretation aller Daten sowie die Reaktion auf mögliche Sicherheitsvorfälle.	ESET MDR Ultimate	✓			
	Mit dem KI-gestützten Managed Detection & Response Service haben auch Unternehmen mit weniger finanziellen Ressourcen die Möglichkeit, von der Expertise der ESET Spezialisten zu profitieren. Durch die Anbindung an das ESET-eigene Security Information and Event Management (SIEM) Tool wird ESET Inspect mit den nötigen Daten versorgt, um automatisiert auf verdächtige Aktivitäten innerhalb der Unternehmensumgebung zu reagieren.	ESET MDR		✓		
3. Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement,	ESET bietet keine spezielle Backup-Management-Lösung.					
	ESET Experten übernehmen für Sie den operativen Betrieb Ihrer ESET Inspect Instanz – dazu gehört auch die Reaktion auf akute Vorfälle, einschließlich der Eindämmung und Isolierung einer Bedrohung – und unterstützen Sie so dabei, den Betrieb im Falle eines Vorfalls aufrecht zu erhalten.	ESET MDR Ultimate	✓			

BSIG im Wortlaut	Unser Ansatz für eine mögliche Umsetzung	ESET Lösung	ESET PROTECT Bundles			
			MDR Ultimate	MDR	Elite	Complete
4. Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zu unmittelbaren Anbietern oder Diensteanbietern,	Prävention ist unsere Expertise. ESET Sicherheitslösungen erkennen und wehren Bedrohungen wie Viren, Ransomware, Phishing oder Spam zuverlässig ab[1] und verhindern damit auch deren Ausbreitung auf andere Organisationen. Unsere Schutzlösungen für Clients, Mobilgeräte, Server und Cloud-Anwendungen bilden die Basis. Ergänzt werden sie durch unsere cloudbasierte Sandboxing-Lösung ESET LiveGuard® Advanced, die selbst Zero-Days zuverlässig erkennt.	ESET Endpoint Security | ESET Server Security | ESET Mail Security | ESET Security for Microsoft SharePoint Server ESET LiveGuard® Advanced	✓	✓	✓	✓
5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen,	Der Großteil unserer Produkte und Services ist nach ISO 27001 und ISO 9001 zertifiziert. Die Zertifizierung umfasst alle Unternehmensprozesse von der sicheren Programmierung bis hin zum Vertrieb. Damit gewährleisten wir ein hohes Maß an Produktqualität sowie Informationssicherheit im eigenen Haus.		✓	✓	✓	✓
	Unsere Schwachstellen- und Patch-Management-Lösung sorgt dafür, dass Sicherheitslücken auf Endgeräten und Servern umgehend erkannt und behoben werden.	ESET Vulnerability & Patch Management	✓	✓	✓	✓
6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Sicherheit in der Informationstechnik,	Dank regelmäßiger, automatisch generierbarer Reports mit relevanten Sicherheitsereignissen und Kennzahlen behalten Sie den Überblick über den Sicherheitsstatus in Ihrem Unternehmensnetzwerk. Hierdurch lässt sich zudem nachverfolgen und belegen, dass festgelegte Schutzmaßnahmen tatsächlich greifen. Darüber hinaus können Sie aus den Erkenntnissen der Reports Maßnahmen zur weiteren Verbesserung Ihres Schutzes ableiten und so Ihr Sicherheitsniveau kontinuierlich steigern.	ESET PROTECT + ESET Inspect	✓	✓	✓	✓*
7. grundlegende Schulungen und Sensibilisierungsmaßnahmen im Bereich der Sicherheit in der Informationstechnik,	Unsere kostenlosen Trainings stärken das Bewusstsein für IT-Sicherheit bei allen Mitarbeitenden in Ihrem Unternehmen.	ESET Cybersecurity Awareness Trainings	✓	✓	✓	✓

[1] Aktueller Test: https://www.av-comparatives.org/tests/business-security-test-2025-august-november/

* ohne ESET Inspect

BSIG im Wortlaut	Unser Ansatz für eine mögliche Umsetzung	ESET Lösung	ESET PROTECT Bundles			
			MDR Ultimate	MDR	Elite	Complete
8. Konzepte und Prozesse für den Einsatz von kryptographischen Verfahren,	Unsere inhouse entwickelte und patentierte Festplattenverschlüsselung mit Pre-Boot-Authentifizierung bietet zuverlässigen Schutz für ruhende Daten. Selbst bei Verlust oder Diebstahl eines Geräts oder im Falle des Austritts eines Mitarbeiters werden unautorisierte Zugriffe auf die Daten verhindert und die Informationssicherheit gewährleistet.	ESET Full Disk Encryption	✓	✓	✓	✓
	Mit der Endpoint-Verschlüsselungslösung können Sie neben ruhenden Daten auch Daten in Bewegung zuverlässig absichern. Hierzu zählen neben E-Mails und Anhängen insbesondere externe Medien wie USB-Sticks. Diese Lösung ist perfekt zugeschnitten auf Organisationen mit besonderen Verschlüsselungsanforderungen sowie expliziten Richtlinien für den Einsatz gemeinsam genutzter Geräte.	ESET Endpoint Encryption	*	*	*	*
9. Erstellung von Konzepten für die Sicherheit des Personals, die Zugriffskontrolle und für die Verwaltung von IKT-Systemen, -Produkten und -Prozessen,	Für alle Nutzer im Netzwerk können über dynamisch festlegbare Gerätegruppen ganz unkompliziert verschiedene Maßnahmen durchgesetzt werden, z.B. automatisierte Updates der Sicherheitssoftware auf den Endpoints oder die Installation bzw. Deinstallation von Drittanbieter-Software. Für alle Administratoren bzw. Nutzer der Management-Konsole lassen sich spezifische Rechte für den Zugriff und die Verwaltungsmöglichkeiten festlegen.	ESET PROTECT	✓	✓	✓	✓
	Mit unserer Endpoint-Verschlüsselungslösung können Sie Zugriffsrechte bis auf die Dateiebene festlegen. So verhindern Sie unbefugte Zugriffe auf besonders schützenswerte Daten wie z.B. Konstruktionspläne.	ESET Endpoint Encryption	*	*	*	*
10. Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.	Unsere unkomplizierte und einfach zu implementierende Multi-Faktor-Authentifizierung funktioniert mobilbasiert und schützt den Zugang zu gemeinsam genutzten Systemen (Windows & Server Logins, Microsoft-Dienste wie ADFS oder OWA sowie SAML, FIDO, VPNs und RADIUS-basierte Dienste). Auf Wunsch lassen sich mittels biometrischen FIDO-Sticks sogar beinahe passwortlose Umgebungen realisieren.	ESET Secure Authentication	✓	✓	✓	
	Mit unserer Schutzlösung für Mailserver sichern Unternehmen ihre E-Mail-Kommunikation zuverlässig ab. Die Lösung schützt den Host selbst und verhindert so, dass digitale Bedrohungen wie Spam oder Phishing die Posteingänge der Nutzer erreichen.	ESET Mail Security	✓	✓	✓	✓
	Sofern Sie Microsoft 365 oder Google Workspace Anwendungen nutzen, sollten Sie diese zusätzlich schützen. Die Kombination aus Spam-Filter, Malware-Scanner, Anti-Phishing und Cloud Sandboxing in unserer Lösung sichert Ihre Unternehmenskommunikation, Zusammenarbeit und den vorhandenen Cloud-Speicher nachhaltig ab.	ESET Cloud Office Security	✓	✓	✓	✓

* separat buchbar

Stand: Mai 2026 | Artikelnummer: M_PRINT2026_12

3 VON ÜBER 500.000 ZUFRIEDENEN KUNDEN

BVB 09 CHAMPION PARTNER

Seit 2019 ein starkes Team auf dem Platz und digital

KLINIKUM LANDSHUT

Seit 2022 durch ESET geschützt
Mehr als 1.450 Postfächer

T

ISP Security Partner seit 2008
2 Millionen Kunden

BEWÄHRT

Secur|Ty made in EU
Trust Seal www.SekturitZofTheme

ESET wurde das Vertrauenssiegel „IT Security made in EU" verliehen

SGS ISO 9001 SYSTEM CERTIFICATION
SGS ISO/IEC 27001 SYSTEM CERTIFICATION

Unsere Lösungen sind nach den Qualitäts- und Informationssicherheitsstandards ISO 9001:2015 und ISO/IEC 27001:2022 zertifiziert

NATO OTAN

In strategischer Partnerschaft

ESET IN ZAHLEN

110.000.000+
Geschützte Nutzer weltweit

500.000+
Geschützte Unternehmen

178
Länder & Regionen

12
Forschungs- und Entwicklungszentren weltweit

ÜBER ESET

Als europäischer Hersteller mit mehr als 35 Jahren Erfahrung bietet ESET ein breites Portfolio an Sicherheitslösungen für jede Organisationsgröße. Wir schützen betriebssystemübergreifend sämtliche Endpoints und Server mit einer vielfach ausgezeichneten mehrschichtigen Technologie und halten Ihre Infrastruktur mithilfe von Cloud Sandboxing frei von Zero-Day-Bedrohungen. Mittels Multi-Faktor-Authentifizierung und zertifizierter Verschlüsselungslösungen unterstützen wir Sie bei der Umsetzung von Datenschutzbestimmungen sowie Compliance-Maßnahmen.

Unsere Extended Detection and Response-Lösung, dedizierte Services wie z.B. Managed Detection and Response und Frühwarnsysteme in Form von Threat Intelligence ergänzen das Angebot im Hinblick auf Incident Management sowie den Schutz vor gezielter Cyberkriminalität und APTs. Dabei setzt ESET nicht allein auf modernste KI-Technologie, sondern kombiniert Erkenntnisse aus der cloudbasierten Reputationsdatenbank ESET LiveGrid® mit Machine Learning und menschlicher Expertise, um Ihnen den besten Schutz zu gewährleisten.

eset® BLOG

ESET Deutschland GmbH
Spitzweidenweg 32 | 07743 Jena | Tel.: +49 3641 3114 200

ESET.DE | ESET.AT | ESET.CH

Cybersecurity
Progress. Protected.

MADE IN EU

ESET.DE/NIS2

Stand: 07/2026 | Druck: 07/2026 | Artikelnummer: M_PRINT2026_14

WHITEPAPER

NIS2 und die Lieferkette



Welche Anforderungen kommen auf Zulieferer, Dienstleister und andere Akteure der Supply Chain zu?

ESET Cybersecurity
Progress. Protected.

ESET.DE/NIS2

Cybersecurity
Progress. Protected.

Einleitung

In der heutigen digitalen Welt ist IT-Sicherheit ein entscheidender Faktor für Organisationen jeder Größe und Branche. Die steigende Bedeutung wird durch die Richtlinie NIS 2.0 (Network and Information Systems Directive 2.0) auf europäischer Ebene unterstrichen und weiter verstärkt.

Neben den gesetzlichen Anforderungen spielt die Risikominimierung eine zentrale Rolle für alle Organisationen, um nicht in eine bedrohliche finanzielle oder existenzielle Schieflage nach einem Cyberangriff zu geraten. Unabhängig von bevorstehenden Gesetzesänderungen müssen Unternehmen und Institutionen bereits heute angemessene Maßnahmen ergreifen, um sich vor digitalen Attacken zu schützen. Dahingehende Pflichten der Geschäftsleiter bestehen bereits heute. Der hierbei geforderte Stand der Technik ist jedoch eine oftmals als oft vage wahrgenommene Anforderung, was aus rechtlicher Sicht unzutreffend ist. Die Bestimmung der inhaltlichen Anforderungen ist im Einzelfall indes aufwändig und unterbleibt aus diesem Grund vielfach.

Es ist von großer Bedeutung, dass Organisationen die immense gesellschaftliche und geopolitische Relevanz der IT-Sicherheit verstehen und die Konsequenzen ihres Handelns oder Nichthandelns erkennen. Die bisher in den Medien erschienenen Sicherheitsvorfälle verdeutlichen den dringenden Handlungsbedarf, der den Gesetzgeber zum Eingreifen veranlasst hat. Und das ist sicherlich bloß der berüchtigte Eisberg, die Dunkelziffer der Vorfälle dürfte deutlich größer sein. Die bloße Eigenmotivation zur Schadensprävention hat sich als unzureichend erwiesen.

Allgemeine Gesetze zur ordnungsgemäßen Geschäftsorganisation und Sorgfalt haben Unternehmen nicht genug Druck gemacht, angemessene IT-Sicherheitsmaßnahmen zu ergreifen. Die bereits existierenden Anforderungen wurden oft ignoriert oder nur unzureichend umgesetzt. Die Richtlinie NIS 2.0 adressiert diesen Bedarf und bringt spezifische gesetzliche Vorgaben für die IT-Sicherheit, die für einen erheblichen Teil der Wirtschaft und zahlreiche öffentliche Stellen gelten werden.

Dieses Whitepaper widmet sich vor allem der Frage, welche Unternehmen und Organisationen voraussichtlich von den neuen gesetzlichen Vorgaben betroffen sein werden. Es ist ratsam, sofort entsprechende Maßnahmen zu ergreifen und nicht auf den Erlass des deutschen Gesetzes zu warten, das die Vorgaben der Richtlinie NIS 2.0 für Unternehmen in Deutschland verbindlich machen wird. Die Richtlinie fordert von Deutschland, diese Vorschriften bis zum 17. Oktober 2024 zu erlassen und ab dem 18. Oktober 2024 national anzuwenden.

Durch proaktive Maßnahmen und die Auswahl einer geeigneten Strategie kann eine erfolgreiche Risikominimierung zeitnah erreicht werden. Angesichts der üblicherweise langen Einführungszeiten von IT-Projekten ist es jedoch allen Unternehmen dringend zu empfehlen, entsprechende Initiativen zur Implementierung angemessener Maßnahmen umgehend zu ergreifen.

Ich hoffe, Sie erhalten beim Lesen einen informativen Einblick in das Thema.

Stefan Sander

Fachanwalt für IT-Recht
Datenschutzbeauftragter (TÜV)

SDS Rechtsanwälte Sander
Schöning PartG mbB

Autor:
Stefan Sander / SDS Rechtsanwälte
Sander Schöning PartG mbB
Rechtsanwalt - Fachanwalt für IT-Recht -
Datenschutzbeauftragter (TÜV)

Co-Autor:
Michael Klatte / ESET Deutschland GmbH
PR Manager

Auflage 1; März 2024

ESET.DE/NIS2

Inhaltsverzeichnis

1. Der Stand der Dinge bei NIS2 4

Von der Idee zur EU-Richtlinie 4
Aktuelle rechtliche Unsicherheit – Welches Gesetz gilt eigentlich und ab wann? 4
Sicherheit in der Unsicherheit 5

2. Diese Organisationen werden definitiv betroffen sein 6

Über wesentliche und wichtige Einrichtungen – oder: Die Adressaten des Gesetzes 6
Zugehörigkeit zu einem bestimmten Sektor 8
Erstes Kriterium 8
Zweites Kriterium 10
So werden wirtschaftliche Kennzahlen ermittelt 11

3. Was bedeutet das für die Unternehmen der Lieferkette? 12

Sind wir verpflichtet, nur weil wir der Lieferkette angehören? 12
Umsetzung von NIS2 erschafft neues Potential für den IT-Markt 14
Neues Marktpotenzial winkt dem Channel 14

4. Da kommt was auf Sie zu: Gesetzliche Pflichten für NIS2 15

Governance 15
Risikomanagementmaßnahmen 16
Berichtspflichten 17

5. Fazit 18

Wir unterstützen Sie bei der Umsetzung der NIS2-Richtlinie 18

Anhang: ESET Lösungen für NIS2-Compliance 19

Cybersecurity
Progress. Protected.

1. Der Stand der Dinge bei NIS2

Von der Idee zur EU-Richtlinie

In einer Zeit, in der viele europäische Vorschriften oft kontrovers diskutiert werden, finden einige von ihnen jedoch breite Zustimmung. Während einige Regelungen der Europäischen Union – wie beispielsweise die Vorschriften zur Krümmung von Bananen oder Lautstärke von Dudelsäcken – fragwürdig erscheinen mögen, hat die EU in den Bereichen Datenschutz und Cybersicherheit Standards gesetzt. Die Datenschutz-Grundverordnung (DS-GVO) führte neue Maßstäbe für den Schutz personenbezogener Daten ein. Die jüngste Aktualisierung der „Netzwerk- und Informationssicherheit"-Richtlinie (NIS2) schickt sich an, die Fähigkeiten zur Cyberabwehr in der Fläche erheblich zu erhöhen.

Was ursprünglich mit der Idee startete, den Schutz kritischer Infrastrukturen zu verbessern, erwies sich aufgrund der rapiden, fortschreitenden Entwicklungen – insbesondere der Bedrohungslage – schnell als überarbeitungsbedürftig. Die gesetzlichen Regelungen von 2016 wurden Ende 2020 dahingehend überprüft, dass die anfänglichen Anforderungen den aktuellen Bedrohungen nicht mehr gerecht wurden. Ende 2022 wurde das Gesetzgebungsverfahren der Europäischen Union abgeschlossen, welches nicht nur konkretere und umfassendere inhaltliche Vorgaben zur IT-Sicherheit mit sich brachte, sondern auch den Geltungsbereich des Gesetzes erheblich erweiterte. Während zuvor ausschließlich Betreiber kritischer Infrastrukturen betroffen waren, verlangt die künftige Rechtslage gemäß der Richtlinie NIS 2.0 auch von mittleren Unternehmen zahlreicher Branchen, angemessene technische und organisatorische Maßnahmen (TOM) zu ergreifen – und das bis ins Detail.

Aktuelle rechtliche Unsicherheit
– Welches Gesetz gilt eigentlich und ab wann?

Die Richtlinie (EU) 2022/2555 („**NIS2**") ist ein von der Europäischen Union verabschiedetes Gesetz. Es trat am 17. Januar 2023 in Kraft, jedoch begründet es nicht unmittelbar die besagten gesetzlichen Pflichten für Unternehmen in Deutschland. Hätte die EU dieses Gesetz als Verordnung und nicht als Richtlinie erlassen, wäre es direkt und zwingend in allen Mitgliedsstaaten der EU anwendbar, und die dort ansässigen Unternehmen wären direkt betroffen. Es hätte sogar Vorrang vor etwaigen nationalen Gesetzen der Mitgliedsstaaten, falls diese andere inhaltliche Aussagen enthielten. Jedoch ist es keine Verordnung, sondern eine Richtlinie geworden.

Konkrete gesetzliche Vorgaben zur IT-Sicherheit, die in manchen Details durchaus anspruchsvoll umzusetzen sein werden (wie etwa die Erfüllung von Berichtspflichten bei erheblichen Sicherheitsvorfällen innerhalb von 24 Stunden mit erheblicher Detailtiefe), verdienen bereits im Vorfeld ihres Inkrafttretens Aufmerksamkeit. Welche spezifischen gesetzlichen Vorgaben jedoch aufgrund der NIS2-Richtlinie in Deutschland erlassen werden und welche Unternehmen letztendlich konkret verpflichtet sein werden, ist zum jetzigen Zeitpunkt nicht abschließend abzuschätzen.

Denn ein derartiges **deutsches Gesetz** ist noch nicht vom Gesetzgeber verabschiedet.

Sicherheit in der Unsicherheit

Als Gesetz der EU richtet sich die NIS2-Richtlinie wie alle Richtlinien der EU ausschließlich an die Mitgliedsstaaten der EU, was bedeutet, dass es den deutschen Staat insgesamt betrifft. Deutschland ist verpflichtet, seine Gesetze so anzupassen, dass sie mit den Inhalten der NIS2-Richtlinie übereinstimmen. Offiziell trägt das Gesetz den Titel „Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union". Die Bezeichnung „NIS2" ergibt sich lediglich aus dem Zusammenhang, da NIS2 die ältere Richtlinie (EU) 2016/1148 aufhebt und durch inhaltlich überarbeitete, strengere Regelungen ersetzt. Die Richtlinie von 2016 wiederum trug den Titel „Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union" (NIS-Richtlinie).

Die Verpflichtung Deutschlands zur Umsetzung der Richtlinie in nationales Recht wurde mit dem Inkrafttreten der NIS2-Richtlinie am 17. Januar 2023 begründet, wofür bestimmte Fristen festgelegt wurden. Bis zum 17. Oktober 2024 müssen alle EU-Mitgliedstaaten die erforderlichen Vorschriften erlassen und veröffentlichen, um den Anforderungen der Richtlinie zu entsprechen. Gemäß der Richtlinie müssen die Mitgliedsstaaten diese Vorschriften ab dem **18. Oktober 2024** anwenden.

Die derzeitige rechtliche Unsicherheit besteht darin, dass die NIS2-Richtlinie den Mitgliedstaaten nicht verbietet, strengere Bestimmungen zu erlassen oder beizubehalten, die ein höheres Niveau der Cybersicherheit gewährleisten, solange diese Bestimmungen mit den Verpflichtungen der Mitgliedstaaten gemäß dem Unionsrecht, insbesondere der NIS2 Richtlinie, im Einklang stehen. Deutschland hat also die Möglichkeit, im eigenen Gesetz strengere Anforderungen festzulegen und/oder den Kreis derjenigen, die von den gesetzlichen Pflichten erfasst werden, zu erweitern.

Im Umkehrschluss ergibt sich aus Artikel 5 der NIS2-Richtlinie zur **Mindestharmonisierung** in der EU, dass Unternehmen in Deutschland sich bereits darauf vorbereiten können, zumindest mit den Inhalten der Richtlinie konfrontiert zu werden. Mindestens diejenigen Unternehmen, die gemäß den Vorgaben der Richtlinie von den nationalen Gesetzen adressiert werden müssen, werden den entsprechenden Verpflichtungen unterliegen. Für diesen Kreis der sog. „Normadressaten" steht bereits fest, dass sie ab dem Zeitpunkt der Verpflichtung zur Anwendung der Vorschriften die inhaltlichen Pflichten erfüllen müssen, die zumindest minimal vorgesehen sind.

Wenn also im Zusammenhang mit NIS2 oder dem deutschen Umsetzungsgesetz (welches noch nicht existiert) von den zukünftigen Normadressaten heute die Frage gestellt wird, welchen Übergangszeitraum das deutsche Gesetz haben wird – innerhalb dessen sich diese Unternehmen intern anpassen können und die besagten IT-Einführungsprojekte beginnen und erfolgreich abschließen können – ist gemäß Artikel 41 Absatz 1 Satz 2 der NIS2-Richtlinie zu antworten:

Der **Übergangszeitraum** ist die Zeit, die jetzt verstreicht und **am 18. Oktober 2024 endet**.

2. Diese Organisationen
werden definitiv betroffen sein

Über wesentliche und wichtige Einrichtungen – oder: Die Adressaten des Gesetzes

Die zukünftige deutsche Rechtslage wird zumindest die Unternehmen verpflichten, die den Kriterien entsprechen, die die NIS2-Richtlinie in ihren Artikeln 2 und 3 zwingend vorschreibt. Dabei spricht die Richtlinie von „wesentlichen und wichtigen Einrichtungen", in Deutschland werden jedoch Entwürfe für ein Umsetzungsgesetz diskutiert, die diese beiden Kategorien als "besonders wichtige Einrichtungen und wichtige Einrichtungen" bezeichnen. Der aktuell bekannte Entwurfsstand ist der Referentenentwurf des Bundesministeriums des Innern und für Heimat (BMI) vom 22.12.2023. Über diesen Entwurf besteht aber schon allein innerhalb der Bundesregierung, also zwischen Ressorts, noch keine Einigkeit – geschweige denn es hätte eine politische Diskussion über diesen im Bundestag auch nur begonnen, welche auch noch zu führen sein wird.

Einen ersten, kurzen Überblick gibt die folgende Abbildung. Der Kreis der Normadressaten, also der betroffenen „Einrichtungen", wird durch eine Tätigkeit in einem bestimmten Sektor sowie durch zwei spezifische Eigenschaften konkretisiert, von denen beide erfüllt sein müssen. Auf diese beiden Eigenschaften, wirtschaftliche Kennzahlen sowie die Größe des Unternehmens, gehen wir in diesem Kapitel später detailliert ein.

Die aktuelle rechtliche Situation in Deutschland, die noch durch die mittlerweile aufgehobene ältere Richtlinie (EU) 2016/1148 (NIS-Richtlinie) geprägt ist, unterscheidet sich von der zukünftigen Rechtslage. Die erwartete Gesetzesänderung betrifft den auf europäischer Ebene geänderten Anknüpfungspunkt. Aktuell richten sich die gesetzlichen Anforderungen an Betreiber kritischer Infrastrukturen. Ob eine Infrastruktur „kritisch" ist, wird anhand von Schwellenwerten bestimmt, die den Versorgungsgrad für die Bevölkerung berücksichtigen und sich auf eine Referenzgruppe von 500.000 Bürgern beziehen. Die fragmentierten Schwellenwert-Tabellen für verschiedene Arten von Anlagen werden in Bezug auf die spezifische Rechtslage für die IT-Sicherheit durch einheitliche Regeln ersetzt. Zukünftig werden die gesetzlichen Verpflichtungen zur IT-Sicherheit nicht mehr davon abhängig sein, ob eine von einer Einrichtung betriebene Anlage für die Versorgungssicherheit der Bevölkerung als kritisch eingestuft wird. Stattdessen werden ganze Einrichtungen anhand wirtschaftlicher Kennzahlen und der Größe der Einrichtung zu den Adressaten der Verpflichtungen.

Die Regelungen für kritische Infrastrukturen bleiben übrigens erhalten. Diese werden auch weiterhin als Einrichtungen oder Betreiber von Anlagen oder Teilen davon definiert, die hinsichtlich ihres Versorgungsgrads für die Bevölkerung als „kritisch" eingestuft werden. Diese Regelungen betreffen die physische Sicherheit kritischer Infrastrukturen und die entsprechenden Pflichten der Betreiber.

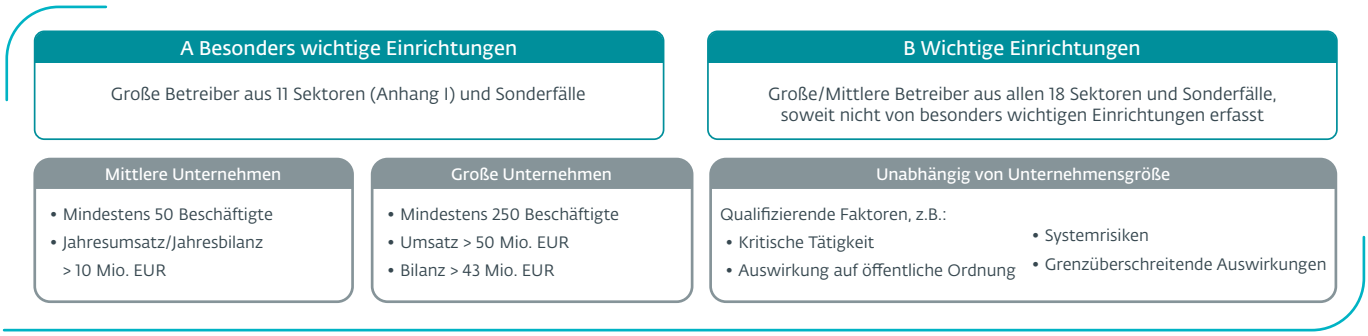


Abb. 1: Schwellenwerte und Definitionen nach NIS-2-Richtlinie

Erstes Kriterium

Zugehörigkeit zu einem bestimmten Sektor

Gemäß der NIS2-Richtlinie werden als „wesentliche" Einrichtungen (in Deutschland demnächst wohl „besonders wichtige Einrichtungen") die Einrichtungen der in Anhang I der Richtlinie aufgeführten Art betrachtet, die auch das zweite Kriterium erfüllen (siehe unten). Darüber hinaus gibt es in Artikel 3 der NIS2-Richtlinie einige Sonderfälle die, ohne weitere Kriterien zu erfüllen, auch zu dieser Kategorie von Einrichtungen gehören, darunter die Betreiber kritischer Infrastrukturen. Diese werden, als Teilmenge der „wesentlichen" bzw. „besonders wichtigen" Einrichtungen, in gleichem Umfang wie die anderen Einrichtungen dieser Kategorie mit Pflichten zur IT-Sicherheit belegt.

Als (nur) „wichtige" Einrichtungen betrachtet die NIS2-Richtlinie (in Deutschland künftig wohl „wichtige Einrichtungen") die Einrichtungen der in Anhang I oder II der Richtlinie aufgeführten Art, die auch das zweite Kriterium erfüllen (siehe unten) und die nicht bereits als „wesentliche" Einrichtungen im Sinne der Richtlinie gelten.

Sektoren nach Anhang I	Sektoren nach Anhang II
Energie	Post- und Kurierdienste
Verkehr und Transport	Abfallwirtschaft
Bankwesen	Produktion, Herstellung und Handel mit chemischen Stoffen
Finanzmärkte	Produktion, Verarbeitung und Handel von Lebensmitteln
Gesundheitswesen	Verarbeitendes Gewerbe/Herstellung von Waren
Trinkwasser	Anbieter digitaler Dienste
Abwasser	Forschungseinrichtungen
Digitale Infrastruktur	
ICT* Service Management (Managed Service Provider - MSP)	
Öffentliche Verwaltung	
Weltraum	

Abb. 2: Sektorenübersicht nach NIS2-Richtlinie

* Information and Communication Technology

In beiden Anhängen der NIS2-Richtlinie wird die Zugehörigkeit einer Einrichtung zu einem der Sektoren noch etwas weiter präzisiert (in vorstehender Abbildung ausgelassen), was hier anhand zweier Beispiele betrachtet werden soll. IT-Dienstleister und Zulieferer werden es geahnt haben: Sie erfüllen allein durch ihre Branchenzugehörigkeit schon einmal eine der Anforderungen der NIS2-Richtlinie. Sektor **Nr. 9 aus Anhang I**, welcher in der deutschen Sprachfassung mit „Verwaltung von IKT-Diensten (Business-to-Business)" bezeichnet wird, gliedert sich auf in die Anbieter verwalteter Dienste und die Anbieter verwalteter Sicherheitsdienste. Diese beiden Begriffe haben für Zwecke der NIS2-Richtlinie jeweils eine feststehende Bedeutung. Hier werden gezielt Managed Service Provider (MSP) angesprochen.

Gemäß Artikel 6 Nummer 39 der NIS2-Richtlinie wird ein **„Anbieter verwalteter Dienste"** als eine Einrichtung definiert, die Dienste im Zusammenhang mit der Installation, der Verwaltung, dem Betrieb oder der Wartung von IKT-Produkten, Netzen, Infrastruktur, Anwendungen oder jeglicher anderer Netz- und Informationssysteme durch Unterstützung oder aktive Verwaltung erbringt, sei es in den Räumlichkeiten der Kunden oder aus der Ferne.

Gemäß Artikel 6 Nummer 40 der NIS2-Richtlinie wird ein **„Anbieter verwalteter Sicherheitsdienste"** als ein Anbieter verwalteter Dienste (siehe oben, d. h. die Sprache ist von einer Teilmenge) definiert, der Unterstützung für Tätigkeiten im Zusammenhang mit dem Risikomanagement im Bereich der Cybersicherheit durchführt oder erbringt. Beispiele hierfür sind Dienstleister, die Services wie Managed Detection and Response (MDR) anbieten oder allgemeine Managed Security Services Provider (MSSP) sind.

Selbstverständlich gibt es auch andere Bereiche, die nicht in erster Linie mit IT in Zusammenhang stehen. Ein Beispiel wäre die Automobilindustrie, die einen Teil des Sektors mit der Nr. 5 in Anhang II ausmacht. In der deutschen Sprachfassung ist der Sektor betitelt mit „Verarbeitendes Gewerbe/Herstellung von Waren" und gliedert sich in sechs Bereiche auf. Einer davon ist die Herstellung von Kraftwagen und Kraftwagenteilen, d.h. gemeint ist der Wirtschaftszweig, in den Automobilhersteller und deren Zulieferer fallen. Die Lieferkette ist also nicht „als solche" vom Gesetzgeber adressiert, sondern die Betroffenheit der Unternehmen aus der Lieferkette ergibt sich über ihre eigene Zugehörigkeit zu einem bestimmten „Wirtschaftszweig". Darüber hinaus kommt „die Lieferkette" nochmals ins Spiel, bei den konkret zu ergreifenden Maßnahmen, worauf weiter unten eingegangen wird.

Zweites Kriterium

Wirtschaftliche Kennzahlen der Einrichtung („size cap")

Neben der Zugehörigkeit zu einem der Sektoren enthält die NIS2-Richtlinie als zweites Kriterium klare Vorgaben, ab wann ein Unternehmen unter die Richtlinie fällt. Politisch gewollt war es, dass bereits **„mittlere Unternehmen"** von den **Verpflichtungen** erfasst sein sollen.

Es stellt sich die Frage, wer oder was als „mittleres Unternehmen" oder als „großes Unternehmen" überhaupt bezeichnet wird. Die Antwort darauf gibt der im Laufe der Jahre immer wieder überarbeitete Benutzerleitfaden zur **Definition von KMU** der Europäischen Kommission, Generaldirektion Binnenmarkt, Industrie, Unternehmertum und KMU[1]. Diese Definition wird von der NIS2 Richtlinie ausdrücklich in Bezug genommen und ist damit für Deutschland bei Umsetzung der Richtlinie in nationales Recht eine zwingende Vorgabe. Die Anzahl der Mitarbeiter und eine wirtschaftliche Kennzahl, der Jahresumsatz oder die Jahresbilanzsumme entscheiden darüber, ob das Unternehmen NIS2 befolgen muss oder nicht. Konkret formulierte der europäische Gesetzgeber: Die NIS2-Richtlinie gilt für öffentliche oder private Einrichtungen der in den Anhang I oder II der Richtlinie genannten Art, die nach Artikel 2 des Anhangs der Empfehlung 2003/361/EG (dies ist die europäische KMU-Definition) als mittlere Unternehmen gelten oder die Schwellenwerte für mittlere Unternehmen überschreiten und ihre Dienste in der Union erbringen oder ihre Tätigkeiten dort ausüben. Artikel 3 Absatz 4 des Anhangs dieser Empfehlung gilt nicht für die Zwecke der NIS2-Richtlinie.

Die Betrachtung von Sonderfällen bleibt im Rahmen dieses Whitepapers außen vor. Ist das Unternehmen **mindestens** als **„mittleres Unternehmen"** im Sinne der europäischen KMU-Definition anzusehen oder etwaig größer, ist damit das zweite Kriterium für die Einordnung als „wichtige Einrichtung" erfüllt. Für die – vorrangige – Einordnung als „wesentliche Einrichtung" im Sinne der Richtlinie (in Deutschland demnächst wohl „besonders wichtige Einrichtungen") muss das Unternehmen **größer als** ein **mittleres Unternehmen** im Sinne der europäischen KMU-Definition sein, wobei anzumerken ist, dass dort für solche Unternehmen kein Begriff definiert ist.

Zahlreiche Mittelständler, nicht nur in Deutschland, dürften insbesondere von den Schwellenwerten für die Betriebsgröße von mittleren Unternehmen überrascht sein. Der Bereich der mittleren Unternehmen beginnt bei 50 Mitarbeitern und endet bei 249 Mitarbeitern, wobei der Begriff Mitarbeiter in diesem Kontext eigenständig definiert wird. Das Kriterium umfasst nicht nur Voll- und Teilzeitkräfte, sondern auch Zeitarbeiter sowie Saisonpersonal. Es schließt sogar mitarbeitende Eigentümer sowie Teilhaber ein, die eine regelmäßige Tätigkeit in dem Unternehmen ausüben und finanzielle Vorteile aus dem Unternehmen ziehen.

1 https://www.bafa.de/SharedDocs/Downloads/DE/kmu_handbuch_eu.html

So werden wirtschaftliche Kennzahlen ermittelt

Die europäische KMU-Definition gibt nicht nur die wirtschaftlichen Kennzahlen vor (Anzahl der Mitarbeiter, Jahresumsatz bzw. Jahresbilanzsumme), die zur Beschreibung von KMU dienen, sondern legt darüber hinaus fest, woher diese Zahlen kommen bzw. welche Zahlen zugrunde zu legen sind.

Zur Bestimmung der Einstufung gemäß der KMU-Definition sind **Konsolidierungen** erforderlich, bei denen wirtschaftliche Kennzahlen von sog. „verbundenen Unternehmen" und von sog. „Partnerunternehmen" zusammengefasst werden. Ein Unternehmen wird als eigenständig betrachtet, wenn es weder Beteiligungen an anderen Unternehmen hält noch andere Unternehmen an ihm beteiligt sind. Bei eigenständigen Unternehmen kommt es nur auf die eigenen wirtschaftlichen Kennzahlen an. Die Durchführung der Konsolidierung, einschließlich der Gewichtung, wird im Benutzerleitfaden zur Definition von KMU der Europäischen Kommission, Generaldirektion Binnenmarkt, Industrie, Unternehmertum und KMU ausführlich erläutert (zur Fundstelle, siehe oben). Dort wird nicht nur der vollständige Text der europäischen KMU-Definition bereitgestellt (Anmerkung: Artikel 3 Absatz 4 des Anhangs der Empfehlung gilt nicht für die Zwecke der NIS2-Richtlinie), sondern es werden auch zahlreiche Beispiele zur Veranschaulichung der Konsolidierung erläutert.

3. Was bedeutet das für die Unternehmen der Lieferkette?

Mit der NIS2-Richtlinie und der nationalen Gesetzgebung kommen auf die Lieferkette eine besondere Verantwortung zu. IT-Dienstleister, die als MSP agieren, fallen unter den Sektor 9 des Anhangs I zur NIS2-Richtlinie und kommen daher als „besonders wichtige Einrichtungen" in Betracht. Gerade im Hinblick auf jüngste Sicherheitsvorfälle ist diese Einstufung nicht überraschend. Im Oktober 2023 legte eine Cyberattacke die Verwaltungen und Rathäuser in mehr als 70 Kommunen in NRW lahm. Ziel des Angriffs war das Netzwerk des IT-Dienstleisters Südwestfalen-IT.

Sind wir verpflichtet, nur weil wir der Lieferkette angehören?

Die NIS2-Richtlinie hat keinen dedizierten Anknüpfungspunkt für „Mitglieder einer Lieferkette", soweit es um die Frage geht, welches Unternehmen von den Rechtspflichten zur IT-Sicherheit betroffen werden wird. Jedoch werden durch die umschriebenen Kriterien zahlreiche Unternehmen der Supply Chain erfasst. Was könnte es also für die Lieferkette konkret bedeuten, wenn ein Unternehmen nach allgemeinen, oben beschriebenen Kriterien vom Gesetz adressiert wird?

Die zukünftige deutsche Gesetzeslage wird Unternehmen dazu verpflichten, sich in besonderem Maße gegen Gefahren aus der Lieferkette und die anderen Unternehmen der Lieferkette zu schützen. Es sind Regelungen zu erwarten, die zur Umsetzung angemessener technischer und organisatorischer Maßnahmen (TOM) verpflichten und diese Pflichten für die Gefahrenquelle Lieferkette präzisieren (derartiges wird es nach Maßgabe der NIS2-Richtline geben, dazu weiter unten).

Dass der bloße Umstand, Teil der Lieferkette zu sein, dazu führen kann, allein deswegen zum Kreis derjenigen zu gehören, an den die gesetzlichen Vorgaben zur IT-Sicherheit adressiert sind, ist nicht abwegig. Denn dies ist gegenwärtig der Fall, d.h. die Rechtslage in Deutschland, die derzeit noch gilt, kennt gesetzliche Pflichten zur IT-Sicherheit speziell in Bezug auf Unternehmen, die der Lieferkette angehören. Unternehmen fallen dann in den Anwendungsbereich, wenn sie als Zulieferer wegen ihrer Alleinstellungsmerkmale von wesentlicher Bedeutung für ein anderes Unternehmen sind, sofern dieses andere Unternehmen als ein Unternehmen in besonderem öffentlichen Interesse angesehen wird. Die zukünftige deutsche Gesetzeslage zur IT-Sicherheit nach Maßgabe der NIS2-Richtlinie wird einen solchen Anknüpfungspunkt jedoch aller Voraussicht nach nicht mehr kennen. Denn es gibt keine Sondervorschriften im Regelungskonzept der NIS2-Richtlinie, die Unternehmen allein deshalb zu Normadressaten machen, weil sie Teil der Lieferkette sind, falls jenes Unternehmen, welches beliefert wird, für sich genommen in den Anwendungsbereich fällt. Ein solcher „abgeleiteter" Grund zur Verpflichtung ist nicht vorgesehen. Vielmehr ging der EU-Gesetzgeber davon aus, dass über das zweite Kriterium („size cap") die Anforderungen so niedrig angesetzt wurden, dass alle aus Sicht des Gesetzgebers „relevanten" bzw. aus seiner Sicht regelungsbedürftigen Unternehmen vom Anwendungsbereich der NIS2-Richtlinie erfasst werden. Es gab damit schlicht keinen Bedarf, über einen zusätzlichen Anknüpfungspunkt Supply Chain weitere Unternehmen in den Anwendungsbereich einzubeziehen, ergänzend zu den ohnehin erfassten Unternehmen. Ebenfalls ist jedoch festzustellen, dass es auch keine Ausnahmen für Zulieferer gibt, Unternehmen also etwaig aus dem Kreis der Normadressaten ausgenommen würden, weil sie „nur" Zulieferer sind. Dass der deutsche Gesetzgeber insoweit „konzeptionell" über die Mindestharmonisierung in der EU hinausgehen wird, ist zwar möglich, derzeit aber nicht abzusehen.

Hinsichtlich der Lieferkette im Bereich IT ist festzustellen, dass über die in den Anhängen der NIS2-Richtlinie enthaltenen Formulierung wohl alle Unternehmen „der Lieferkette" erfasst werden sollten. Dies betrifft insbesondere den Bereich, in dem Unternehmen der Supply Chain nicht bloß Vorlieferanten sind, die einen Gegenstand wie z.B. ein halbfertiges Erzeugnis oder eine Maschine verkaufen, sondern die während des Betriebs der IT ihre Leistungen erbringen bzw. gerade der ausgelagerte Betrieb der IT die Leistungserbringung dieser Unternehmen ist (siehe oben, Sektor Nr. 9 aus Anhang I (MSP)).

Auch hinsichtlich der Lieferkette anderer Branchen ist festzustellen, dass nicht nur die (großen) Hersteller (der Endprodukte, wie oben im Beispiel „Kraftwagen") erfasst werden, sondern über den Begriff der Wirtschaftstätigkeit im Sinne der Statistischen Systematik der Wirtschaftszweige regelmäßig auch die Zulieferer der „Big Player" des jeweiligen Sektors miterfasst werden.

Umsetzung von NIS2 erschafft neues Potential für den IT-Markt

Die technische Umsetzung der NIS2-Richtlinie, die Registrierungs- und Meldepflichten und die Einhaltung der weiteren grundsätzlichen Rahmenbedingungen werden viel Geld verschlingen. Allein für Deutschland gehen Experten von einem jährlichen Erfüllungsaufwand von mehr als 1,65 Milliarden Euro aus. Was für die betroffenen Organisationen Kosten sind, könnte man auf der anderen Seite auch als Chance sehen: Hier entsteht ein zusätzliches Marktpotential für Security-Hersteller, IT-Dienstleistungsunternehmen und die Digitalwirtschaft generell. Viele Unternehmen und Institutionen werden sicherheitstechnisch deutlich aufrüsten müssen.

Doch nicht jeder hat die notwendigen personellen Ressourcen parat, um diese Aufgabe aus eigener Kraft stemmen zu können. Ihnen bleibt fast nichts anderes übrig, als auf externe Unterstützung zurückzugreifen. Es entsteht deshalb ein zusätzliches Marktpotential für die Beratungsbranche, für IT-Sicherheitsbeauftragte, für ISMS-Spezialisten und -Auditoren, für Systemintegratoren und nicht zuletzt für Dienstleister, die mit „as-a-Service–Angeboten" auf dem Markt sind.

Dies ist definitiv auch und gerade für IT-Dienstleister ein interessantes Geschäftsfeld. Die Grundidee der NIS2-Richtlinie, erhöhte Cyber-Resilienz der Volkswirtschaft insgesamt, endet nicht an Grenzen. Deshalb sollten Organisationen ihr eigenes Schutzniveau hinterfragen und die Vorschläge zur digitalen Widerstandskraft gründlich durchdenken. So mancher Firmenlenker wird analysieren, dass die eingesetzten Security-Maßnahmen nicht mehr zur (weltweiten) Gefahrenlage passen.

Neues Marktpotenzial winkt dem Channel

Den IT-Dienstleistern, die in der Regel als Trusted Advisor für ihre Kunden fungieren, kommt hier eine besondere Rolle und Verpflichtung zu. Es gilt, Kunden eindringlich auf Defizite hinzuweisen und gemeinsam mit ihnen individuelle und angemessene Lösungen zu entwickeln. Hierbei wird es künftig stärker als in der Vergangenheit nötig sein, über arbeitsteilige Konzepte nachzudenken. Damit ist gemeint, dass ein Unternehmen mit seinen eigenen IT-Ressourcen nur Teile der IT-Sicherheitslösung betreut und darüber hinaus auf kompetente Dienstleister zurückgegriffen wird. Dies können beispielsweise Services wie Endpoint Detection and Response (EDR), Threat Intelligence oder andere professionelle IT-Security Services sein, die sich in ein sinnvolles Gesamtlösungskonzept integrieren lassen. Für den Channel lohnt es sich darüber nachzudenken, mit welchen potenziellen Partnern und Allianzen man sich aufstellen möchte, um das entstehende Marktpotential erschließen und den Kunden angepasste Lösungen und ein angemessenes Schutzniveau bieten zu können.

4. Da kommt was auf Sie zu: Gesetzliche Pflichten für NIS2

Der Gesetzgeber der NIS2-Richtlinie betrachtet IT-Sicherheit als „Chefsache", was sich in der Umsetzung der Richtlinie demnächst expressis verbis auch im deutschen Gesetz wiederfinden wird. Zudem hat er die zu ergreifenden Maßnahmen der IT-Sicherheit deutlich differenzierter als bislang geregelt und dabei auch „die Lieferkette" in den Blick genommen.



Governance

Die Leitungsorgane wesentlicher und wichtiger Einrichtungen werden zukünftig gesetzlich verpflichtet werden, die von diesen Einrichtungen ergriffenen **Risikomanagementmaßnahmen** im Bereich der Cybersicherheit **zu billigen** und **ihre Umsetzung zu überwachen**. Bei Verstößen gegen die Vorgaben zu Risikomanagementmaßnahmen können die Leitungsorgane **persönlich verantwortlich** gemacht werden.

Darüber hinaus werden die Mitglieder der Leitungsorgane an Schulungen teilnehmen müssen – und zwar ausdrücklich per Gesetz. Ziel ist es, dass sie ausreichende Kenntnisse und Fähigkeiten erwerben, um überhaupt die Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste einschätzen und beurteilen zu können.

Risikomanagementmaßnahmen

Wesentliche und wichtige Einrichtungen werden gesetzlich verpflichtet werden, geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen zu ergreifen. Dabei sollen diese Organisationen die Maßnahmen beherrschen und die Auswirkungen von Sicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Bereiche verhindern oder zumindest möglichst gering halten. Wie oben bereits angedeutet, werden die zukünftigen gesetzlichen Vorgaben demnach ausdrücklich (auch) auf die **Gefahrenquelle „Lieferkette"** bezogen sein – **und**, andersherum betrachtet, auch den **Schutz der Lieferkette** verlangen.

Die zu ergreifenden Maßnahmen müssen unter Berücksichtigung des Stands der Technik und gegebenenfalls der einschlägigen europäischen und internationalen Normen sowie unter Berücksichtigung der Kosten der Umsetzung ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist. Die Auswahl der Maßnahmen muss auf einem gefahrenübergreifenden Ansatz beruhen, der darauf abzielt, sowohl die Netz- und Informationssysteme als auch die physische Umwelt dieser Systeme vor Sicherheitsvorfällen und deren Folgen zu schützen.

Letztlich müssen die Maßnahmen zumindest Folgendes umfassen:

a) Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme;

b) Bewältigung von Sicherheitsvorfällen;

c) Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement;

d) Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Dienstean-bietern;

e) Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen;

f) Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit;

g) grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit;

h) Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung;

i) Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen;

j) Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

Berichtspflichten

Wesentliche und wichtige Einrichtungen sind verpflichtet, ihr entsprechendes CSIRT (Computer-Notfallteam) oder gegebenenfalls eine zuständige Behörde unverzüglich über jeden erheblichen Sicherheitsvorfall zu informieren. Unter bestimmten Umständen müssen diese Einrichtungen auch die Empfänger ihrer Dienste, **also die Lieferkette** zumindest nach unten hin, unverzüglich über solche erheblichen Sicherheitsvorfälle benachrichtigen, die die Erbringung des jeweiligen Dienstes beeinträchtigen könnten.

Besonders wichtig ist zu betonen, dass gemäß der NIS2-Richtlinie nach der Frühwarnung (spätestens innerhalb von 24 Stunden) und der Meldung des Sicherheitsvorfalls (spätestens innerhalb von 72 Stunden) eine gesetzliche Verpflichtung zur Erstattung eines Abschlussberichts vorgesehen sein wird. Die NIS2-Richtlinie legt bereits die Mindestinhalte des Abschlussberichts fest, die unter anderem eine detaillierte Beschreibung des Sicherheitsvorfalls, einschließlich seiner Schwere und Auswirkungen, sowie Angaben zur Art der Bedrohung oder der zugrunde liegenden Ursache, die wahrscheinlich den Sicherheitsvorfall ausgelöst hat, umfassen. Bereits für die Meldung des Sicherheitsvorfalls wird eine „erste Bewertung" des Sicherheitsvorfalls sowie gegebenenfalls die Angabe sog. „indicators of compromise" (IOC) verlangt. Typische IOC sind Prüfsummen von Malware-Dateien, Virensignaturen, URLs, IP-Adressen und Domain Name System Records, z. B. von beteiligten Command-and-Control-Servern eines Botnetzes.

Um den Berichtspflichten im Falle eines erheblichen Sicherheitsvorfalls nachkommen zu können, müssen alle wesentlichen und wichtigen Einrichtungen demnach solche Technologien beschaffen und einsetzen, die sie – rein faktisch betrachtet – in die Lage versetzen, die Pflichten erfüllen zu können. Eine entsprechende Vorbereitung ist unerlässlich und umfasst neben den technischen, operativen und organisatorischen Maßnahmen, die Teil der Risikomanagementmaßnahmen sind, auch die Bereitstellung geeigneter Ressourcen bzw. Verwendung geeigneter Technologien. Nur durch eine solche Vorbereitung können die Berichtspflichten im Ernstfall erfüllt werden.

5. Fazit

Die NIS2-Richtlinie zielt darauf ab, die Cybersicherheit in der EU zu stärken, indem sie klare Anforderungen an Unternehmen stellt und die Zusammenarbeit zwischen den Akteuren in der Lieferkette fördert. Die Sicherheit der Supply Chain ist entscheidend, um Cyberangriffe auf kritische Infrastrukturen zu verhindern und die Resilienz des gesamten Systems zu gewährleisten.

Unternehmen, die unter die NIS2-Richtlinie fallen, können Zulieferer und Dienstleister dazu verpflichten, spezifische Sicherheitsmaßnahmen zu ergreifen, um ihre Systeme und Daten zu schützen. Dies bedeutet, dass Unternehmen, die als digitale Diensteanbieter eingestuft sind, ihre Lieferanten und Partner dazu auffordern können, bestimmte Sicherheitsstandards einzuhalten. Beispielsweise kann ein Energieversorgungsunternehmen, das unter die NIS2-Richtlinie fällt, von seinen Lieferanten verlangen, Schutzmaßnahmen gegen Cyberangriffe zu implementieren, um die Integrität und Verfügbarkeit seiner Dienste sicherzustellen. Es ist vor diesem Hintergrund wichtig, dass Unternehmen ihre Lieferanten und Partner aktiv in ihre Sicherheitsstrategien einbeziehen, um die digitale Resilienz zu erhöhen.

Wir unterstützen Sie bei der Umsetzung der NIS2-Richtlinie

Als europäischer Anbieter im Bereich digitaler Sicherheitslösungen helfen wir Ihnen bei der Implementierung und Erfüllung der NIS2-Vorgaben.

Dafür bieten wir verschiedene Lösungen und Möglichkeiten:

- Wissensaustausch über unsere Kanäle wie den Digital Security Guide oder unseren Corporate Blog
- Interaktive Veranstaltungen wie Workshops
- Unterstützung bei der Einhaltung und Umsetzung von NIS2-Maßnahmen
- Bereitstellung von Sicherheitslösungen, die zur Einhaltung von Vorschriften beitragen
- Unsere Spezialisten stehen Ihnen jederzeit zur Verfügung, um Ihre Fragen zu beantworten

Vereinbaren Sie einen Termin mit unseren ESET Experten



Maik Wetzel

Strategischer Experte
Strategic Business Development Director,
ESET Deutschland GmbH

ESET.DE/NIS2KONTAKT



Michael Schröder

Technischer Experte
Manager of Security Business Strategy
ESET Deutschland GmbH

ESET Lösungen für NIS2-Compliance

In Deutschland wurde mit dem NIS-2-Umsetzungsgesetz, das im Dezember 2025 in Kraft trat, unter anderem das BSI-Gesetz (BSIG) grundlegend überarbeitet und erweitert. Von besonderer Bedeutung für viele Unternehmen sind die neu hinzugekommenen Paragraphen zu Risikomanagement (§ 30) und Meldepflichten (§ 32), die nun für deutlich mehr Sektoren und Einrichtungen gelten (siehe § 28). Die folgende Übersicht zeigt unseren Ansatz für eine mögliche Umsetzung der geforderten IT-Sicherheitsmaßnahmen unter Einsatz von ESET Lösungen.

In Österreich wurde das NIS-2-Umsetzungsgesetz im Dezember 2025 veröffentlicht und tritt im Oktober 2026 in Kraft. Weitere Informationen finden Sie ↗hier.

Bitte beachten Sie, dass unsere Inhalte keine rechtliche Beratung ersetzen. Bitte wenden Sie sich für Ihren konkreten Fall an eine Rechtsanwältin oder einen Rechtsanwalt Ihres Vertrauens.

Übrigens: Das BSIG beinhaltet für die unter das Gesetz fallenden privaten und öffentlichen Einrichtungen **umfangreiche Berichtspflichten**. Dazu gehört, dass Einrichtungen laut § 32 Abs. 1 BSIG einen erheblichen Sicherheitsvorfall **innerhalb von 24 Stunden** der zuständigen Behörde melden müssen. **Innerhalb von 72 Stunden** sollen zudem **Kompromittierungsindikatoren** (IoCs) benannt werden und **nach einem Monat soll ein umfassender Abschlussbericht** vorgelegt werden. Bei der Bereitstellung solch umfangreicher Dokumentationen können Extended Detection & Response (XDR) Lösungen wie ESET Inspect unterstützen.

§ 30 Abs. 2 BSIG:

Maßnahmen nach Absatz 1 sollen den Stand der Technik einhalten, die einschlägigen europäischen und internationalen Normen berücksichtigen und müssen auf einem gefahrenübergreifenden Ansatz beruhen. Die Maßnahmen müssen zumindest Folgendes umfassen:

BSIG im Wortlaut	Unser Ansatz für eine mögliche Umsetzung	ESET Lösung	ESET PROTECT Bundles			
			MDR Ultimate	MDR	Elite	Complete
1. Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik,	Wir von ESET bzw. unsere Vertriebspartner unterstützen Sie bei der technischen Bewertung, Erstellung und Umsetzung von passenden IT-Sicherheitskonzepten entsprechend Ihrer Kundenumgebung.		Unter Umständen Bestandteil der Presales-Phase			
	Mit unserer Management-Konsole haben Sie dank Hard- und Software-Inventarisierung Ihre schützenswerten Assets im Blick und verfügen damit über eine zuverlässige Grundlage für die Risikoanalyse sowie die Erstellung Ihres Sicherheitskonzepts.	ESET PROTECT	✓	✓	✓	✓
2. Bewältigung von Sicherheitsvorfällen,	Unser Extended Detection & Response Tool ermöglicht eine umfassende Gefahrensuche und -abwehr. Ereignisse im Netzwerk werden protokolliert und zu Vorfällen zusammengefasst, sodass Sie einen Überblick darüber haben, was in Ihrer IT-Umgebung vor sich geht. So können Sie bei einem Sicherheitsvorfall schnell reagieren. Dank festgelegter Reaktionsmaßnahmen wird das Sicherheitsniveau zudem weiter gesteigert.	ESET Inspect (in Kombination mit ESET PROTECT)	✓	✓	✓	
	ESET Experten übernehmen den operativen Betrieb Ihrer ESET Inspect Instanz und damit die Überprüfung, Auswertung und Interpretation aller Daten sowie die Reaktion auf mögliche Sicherheitsvorfälle.	ESET MDR Ultimate	✓			
	Mit dem KI-gestützten Managed Detection & Response Service haben auch Unternehmen mit weniger finanziellen Ressourcen die Möglichkeit, von der Expertise der ESET Spezialisten zu profitieren. Durch die Anbindung an das ESET-eigene Security Information and Event Management (SIEM) Tool wird ESET Inspect mit den nötigen Daten versorgt, um automatisiert auf verdächtige Aktivitäten innerhalb der Unternehmensumgebung zu reagieren.	ESET MDR		✓		
3. Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement,	ESET bietet keine spezielle Backup-Management-Lösung.					
	ESET Experten übernehmen für Sie den operativen Betrieb Ihrer ESET Inspect Instanz – dazu gehört auch die Reaktion auf akute Vorfälle, einschließlich der Eindämmung und Isolierung einer Bedrohung – und unterstützen Sie so dabei, den Betrieb im Falle eines Vorfalls aufrecht zu erhalten.	ESET MDR Ultimate	✓			

BSIG im Wortlaut	Unser Ansatz für eine mögliche Umsetzung	ESET Lösung	ESET PROTECT Bundles			
			MDR Ultimate	MDR	Elite	Complete
4. Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zu unmittelbaren Anbietern oder Diensteanbietern,	Prävention ist unsere Expertise. ESET Sicherheitslösungen erkennen und wehren Bedrohungen wie Viren, Ransomware, Phishing oder Spam zuverlässig ab[1] und verhindern damit auch deren Ausbreitung auf andere Organisationen. Unsere Schutzlösungen für Clients, Mobilgeräte, Server und Cloud-Anwendungen bilden die Basis. Ergänzt werden sie durch unsere cloudbasierte Sandboxing-Lösung ESET LiveGuard® Advanced, die selbst Zero-Days zuverlässig erkennt.	ESET Endpoint Security | ESET Server Security | ESET Mail Security | ESET Security for Microsoft SharePoint Server ESET LiveGuard® Advanced	✓	✓	✓	✓
5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen,	Der Großteil unserer Produkte und Services ist nach ISO 27001 und ISO 9001 zertifiziert. Die Zertifizierung umfasst alle Unternehmensprozesse von der sicheren Programmierung bis hin zum Vertrieb. Damit gewährleisten wir ein hohes Maß an Produktqualität sowie Informationssicherheit im eigenen Haus.		✓	✓	✓	✓
	Unsere Schwachstellen- und Patch-Management-Lösung sorgt dafür, dass Sicherheitslücken auf Endgeräten und Servern umgehend erkannt und behoben werden.	ESET Vulnerability & Patch Management	✓	✓	✓	✓
6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Sicherheit in der Informationstechnik,	Dank regelmäßiger, automatisch generierbarer Reports mit relevanten Sicherheitsereignissen und Kennzahlen behalten Sie den Überblick über den Sicherheitsstatus in Ihrem Unternehmensnetzwerk. Hierdurch lässt sich zudem nachverfolgen und belegen, dass festgelegte Schutzmaßnahmen tatsächlich greifen. Darüber hinaus können Sie aus den Erkenntnissen der Reports Maßnahmen zur weiteren Verbesserung Ihres Schutzes ableiten und so Ihr Sicherheitsniveau kontinuierlich steigern.	ESET PROTECT + ESET Inspect	✓	✓	✓	✓*
7. grundlegende Schulungen und Sensibilisierungsmaßnahmen im Bereich der Sicherheit in der Informationstechnik,	Unsere kostenlosen Trainings stärken das Bewusstsein für IT-Sicherheit bei allen Mitarbeitenden in Ihrem Unternehmen.	ESET Cybersecurity Awareness Trainings	✓	✓	✓	✓

[1] Aktueller Test: https://www.av-comparatives.org/tests/business-security-test-2025-august-november/

* ohne ESET Inspect

BSIG im Wortlaut	Unser Ansatz für eine mögliche Umsetzung	ESET Lösung	ESET PROTECT Bundles			
			MDR Ultimate	MDR	Elite	Complete
8. Konzepte und Prozesse für den Einsatz von kryptographischen Verfahren,	Unsere inhouse entwickelte und patentierte Festplattenverschlüsselung mit Pre-Boot-Authentifizierung bietet zuverlässigen Schutz für ruhende Daten. Selbst bei Verlust oder Diebstahl eines Geräts oder im Falle des Austritts eines Mitarbeiters werden unautorisierte Zugriffe auf die Daten verhindert und die Informationssicherheit gewährleistet.	ESET Full Disk Encryption	✓	✓	✓	✓
	Mit der Endpoint-Verschlüsselungslösung können Sie neben ruhenden Daten auch Daten in Bewegung zuverlässig absichern. Hierzu zählen neben E-Mails und Anhängen insbesondere externe Medien wie USB-Sticks. Diese Lösung ist perfekt zugeschnitten auf Organisationen mit besonderen Verschlüsselungsanforderungen sowie expliziten Richtlinien für den Einsatz gemeinsam genutzter Geräte.	ESET Endpoint Encryption	*	*	*	*
9. Erstellung von Konzepten für die Sicherheit des Personals, die Zugriffskontrolle und für die Verwaltung von IKT-Systemen, -Produkten und -Prozessen,	Für alle Nutzer im Netzwerk können über dynamisch festlegbare Gerätegruppen ganz unkompliziert verschiedene Maßnahmen durchgesetzt werden, z.B. automatisierte Updates der Sicherheitssoftware auf den Endpoints oder die Installation bzw. Deinstallation von Drittanbieter-Software. Für alle Administratoren bzw. Nutzer der Management-Konsole lassen sich spezifische Rechte für den Zugriff und die Verwaltungsmöglichkeiten festlegen.	ESET PROTECT	✓	✓	✓	✓
	Mit unserer Endpoint-Verschlüsselungslösung können Sie Zugriffsrechte bis auf die Dateiebene festlegen. So verhindern Sie unbefugte Zugriffe auf besonders schützenswerte Daten wie z.B. Konstruktionspläne.	ESET Endpoint Encryption	*	*	*	*
10. Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.	Unsere unkomplizierte und einfach zu implementierende Multi-Faktor-Authentifizierung funktioniert mobilbasiert und schützt den Zugang zu gemeinsam genutzten Systemen (Windows & Server Logins, Microsoft-Dienste wie ADFS oder OWA sowie SAML, FIDO, VPNs und RADIUS-basierte Dienste). Auf Wunsch lassen sich mittels biometrischen FIDO-Sticks sogar beinahe passwortlose Umgebungen realisieren.	ESET Secure Authentication	✓	✓	✓	
	Mit unserer Schutzlösung für Mailserver sichern Unternehmen ihre E-Mail-Kommunikation zuverlässig ab. Die Lösung schützt den Host selbst und verhindert so, dass digitale Bedrohungen wie Spam oder Phishing die Posteingänge der Nutzer erreichen.	ESET Mail Security	✓	✓	✓	✓
	Sofern Sie Microsoft 365 oder Google Workspace Anwendungen nutzen, sollten Sie diese zusätzlich schützen. Die Kombination aus Spam-Filter, Malware-Scanner, Anti-Phishing und Cloud Sandboxing in unserer Lösung sichert Ihre Unternehmenskommunikation, Zusammenarbeit und den vorhandenen Cloud-Speicher nachhaltig ab.	ESET Cloud Office Security	✓	✓	✓	✓

* separat buchbar

3 VON ÜBER 500.000 ZUFRIEDENEN KUNDEN

CHAMPION PARTNER

Seit 2019 ein starkes Team
auf dem Platz und digital

KLINIKUM LANDSHUT

Seit 2022 durch ESET geschützt
Mehr als 1.450 Postfächer

ISP Security Partner seit 2008
2 Millionen Kunden

BEWÄHRT

Trust Seal
www.teletrust.de/itsmie

ESET wurde das Vertrauenssiegel
„IT Security made in EU" verliehen

Unsere Lösungen sind nach den
Qualitäts- und Informations-
sicherheitsstandards ISO 9001:2015 und
ISO/IEC 27001:2022 zertifiziert

In strategischer Partnerschaft

ESET IN ZAHLEN

110.000.000+

Geschützte Nutzer weltweit

178

Länder & Regionen

500.000+

Geschützte Unternehmen

12

Forschungs- und Entwicklungszentren weltweit

ÜBER ESET

Als europäischer Hersteller mit mehr als 35 Jahren Erfahrung bietet ESET ein breites Portfolio an Sicherheitslösungen für jede Organisationsgröße. Wir schützen betriebssystemübergreifend sämtliche Endpoints und Server mit einer vielfach ausgezeichneten mehrschichtigen Technologie und halten Ihre Infrastruktur mithilfe von Cloud Sandboxing frei von Zero-Day-Bedrohungen. Mittels Multi-Faktor-Authentifizierung und zertifizierter Verschlüsselungslösungen unterstützen wir Sie bei der Umsetzung von Datenschutzbestimmungen sowie Compliance-Maßnahmen.

Unsere Extended Detection and Response-Lösung, dedizierte Services wie z.B. Managed Detection and Response und Frühwarnsysteme in Form von Threat Intelligence ergänzen das Angebot im Hinblick auf Incident Management sowie den Schutz vor gezielter Cyberkriminalität und APTs. Dabei setzt ESET nicht allein auf modernste KI-Technologie, sondern kombiniert Erkenntnisse aus der cloudbasierten Reputationsdatenbank ESET LiveGrid® mit Machine Learning und menschlicher Expertise, um Ihnen den besten Schutz zu gewährleisten.

ESET BLOG

ESET Deutschland GmbH
Spitzweidenweg 32 | 07743 Jena | Tel.:+49 3641 3114 200

ESET.DE | ESET.AT | ESET.CH

Cybersecurity
Progress. Protected.

MADE IN EU

ESET.DE/NIS2

Stand: 07/2026 | Druck: 07/2026 | Artikelnummer: M_PRINT2026_14