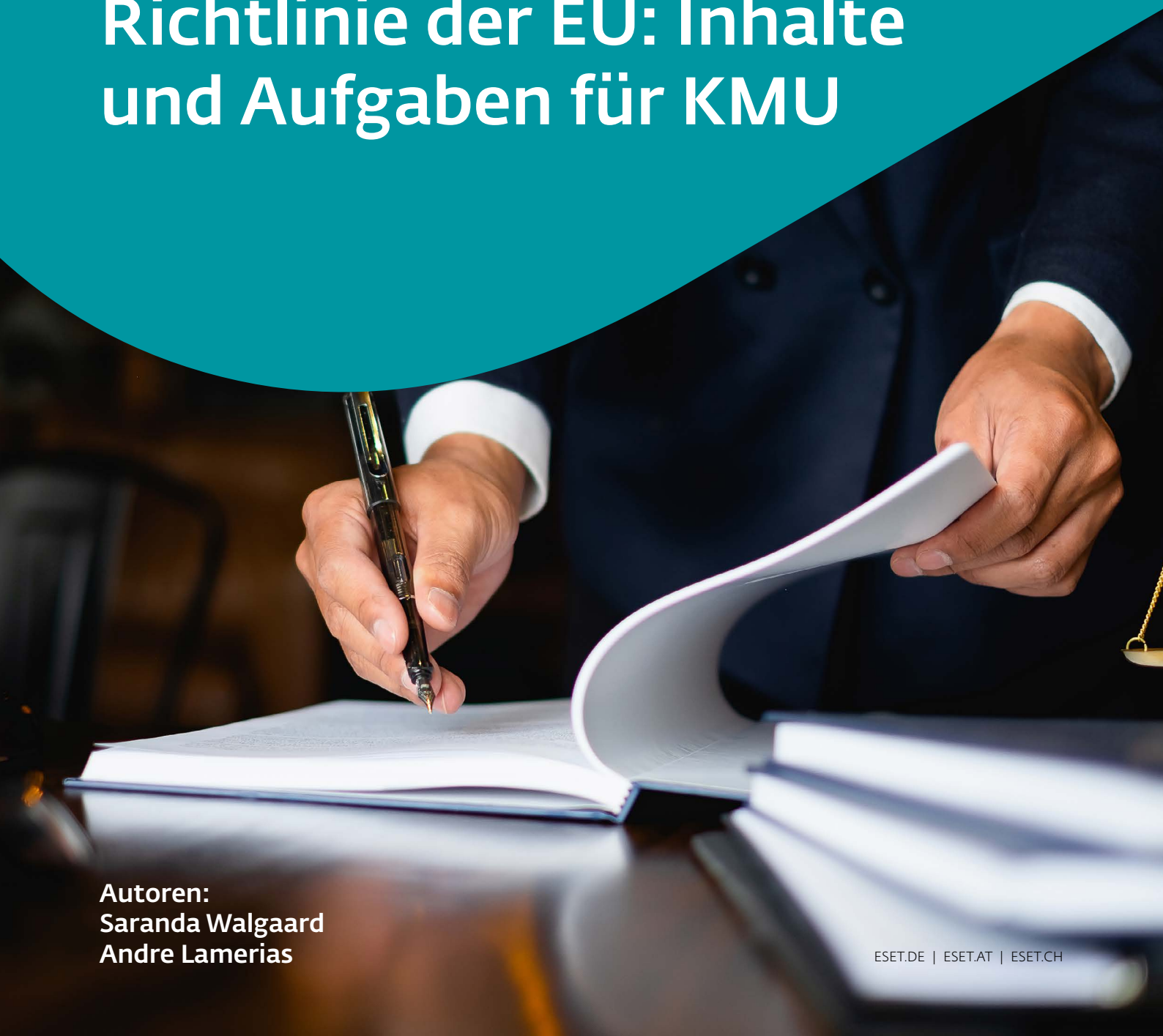
Digital Security
Progress. Protected.

EVERSHEDS SUTHERLAND

NIS2

Die neue Cybersecurity-Richtlinie der EU: Inhalte und Aufgaben für KMU



Autoren:
Saranda Walgaard
Andre Lamerias

ESET.DE | ESET.AT | ESET.CH

INHALT

Was ist die NIS2?

Die NIS2-Richtlinie schafft einen neuen gesetzlichen Rahmen zur Stärkung der Cybersicherheit in der EU. Als aktualisierte Fassung der ursprünglichen NIS (Richtlinie zur Netzwerk- und Informationssicherheit) trat die NIS2 am 16. Januar 2023 in Kraft und verpflichtet Unternehmen kritischer Sektoren wie Energie, Verkehr, Gesundheit, sowie Anbieter digitaler Dienste und verwalteter Sicherheitsdienste, ihr Risikomanagement grundlegend zu überarbeiten. Zusätzlich enthält die NIS2 Regelungen zu neuen Berichtspflichten sowie Strafen und Bußgeldern.

Von NIS zu NIS2: Die Geschichte der Cybersecurity-Gesetzgebung in der EU

Die NIS-Richtlinie von 2016 war die erste EU-weite gesetzliche Vorgabe zur Cybersicherheit. Sie bezog sich hauptsächlich auf zwei Gruppen von Organisationen: „Betreiber wesentlicher Dienste" (Operators of Essential Services OES), z.B. aus den Sektoren Gesundheit, Verkehr und Energie, sowie „Anbieter digitaler Dienste" (Digital Service Providers DSP), z.B. Online-Suchmaschinen, Online-Marktplätze und Anbieter von Cloud-Computing-Diensten. Die NIS-Richtlinie verpflichtete sie, bestimmte Mindestanforderungen zu erfüllen und gravierende Sicherheitsvorfälle zu melden. Dabei blieb es den einzelnen EU-Staaten überlassen, die Richtlinie entsprechend der Anforderungen des jeweiligen Landes umzusetzen.

Die NIS2 schafft nun einen ganz neuen Rahmen, um das Cybersicherheitsniveau in der gesamten EU zu stärken. Als aktualisierte Fassung der ersten Richtlinie zur Netzwerk- und Informationssicherheit trat die NIS2 am 16. Januar 2023 in Kraft und nimmt nicht nur EU-Mitgliedsstaaten in die Pflicht. Auch Organisationen und Unternehmen außerhalb der EU, die besondere Bedeutung für den europäischen Markt haben, werden in der Richtlinie bedacht.

Die NIS2 verpflichtet Unternehmen der sogenannten „Sektoren mit hoher Kritikalität", bestimmte technische und organisatorische Maßnahmen zu ergreifen. Dazu gehören die Reaktion auf Sicherheitsvorfälle, die Absicherung der Lieferkette (Supply Chain Security), Verschlüsselung, die Offenlegung von Schwachstellen, wirksame Risikoanalysen, die Prüfung und Auditierung von Strategien für die Cybersicherheit sowie die Erstellung von Krisenmanagement-Plänen zur Aufrechterhaltung des Betriebs auch im Krisenfall.

Sektoren in der ursprünglichen NIS-Richtlinie

- Gesundheitswesen
- Digitale Infrastruktur
- Verkehr
- Trinkwasserversorgung
- Anbieter digitaler Dienste
- Bank- und Finanzmarkt-infrastrukturen
- Energie

Zusätzliche Sektoren laut NIS2

- Anbieter öffentlicher elektronischer Kommunikationsnetze oder -dienste
- Abwasser- und Abfallwirtschaft
- Herstellung von bestimmten kritischen Produkten (z. B. Arzneimittel, mediz. Geräte und Chemikalien)
- Lebensmittel
- Digitale Dienstleistungen (z.B. Plattformen für Dienste sozialer Netzwerke und Rechenzentrumsdienste)
- Weltraum (z. B. Luft- und Raumfahrt)
- Post- und Kurierdienste
- Öffentliche Verwaltung

Im Fall eines Sicherheitsvorfalls sind die Einrichtungen außerdem verpflichtet, innerhalb von 24 Stunden nach dem Vorfall eine erste Meldung abzusetzen sowie innerhalb von 72 Stunden detaillierte Informationen nachzureichen. Mit der NIS2 werden außerdem Bußgelder für die Nichteinhaltung der Vorschriften eingeführt, einschließlich der Möglichkeit, die Zertifizierung oder Genehmigung für den Geschäftsbetrieb für eine gewisse Zeit zu entziehen sowie leitende Angestellte entsprechend der nationalen Gesetzgebung persönlich haftbar zu machen.

Mit der Richtlinie wird außerdem mit **EU-CyCLONe** (European Cyber Crises Liaison Organization Network) ein europäisches Netzwerk eingerichtet, welches die Zusammenarbeit zwischen den Cybersecurity-Behörden auf Landesebene erleichtern soll. Zudem wird jeder Mitgliedsstaat verpflichtet, eine zentrale Meldestelle für Cybersicherheitsvorfälle zu benennen.

Die NIS2 ist bis zum September 2024 in nationale Gesetze der einzelnen Mitgliedsstaaten umzusetzen und tritt damit dann final in Kraft. Nichtsdestotrotz sind Unternehmen gut beraten, sich bereits jetzt mit den Vorgaben auseinanderzusetzen, um einerseits die Implementierung der Regeln rechtzeitig in die Wege zu leiten. Andererseits hilft eine frühe Auseinandersetzung dabei, verschiedene Methoden im Umgang mit Sicherheitsvorfällen sowie Kontrollmechanismen und Meldeverfahren ausgiebig zu testen, bevor Sanktionen drohen.

Der Verlauf im Überblick

08/2016
NIS-Richtlinie tritt in Kraft

05/2018
Frist für Umsetzung der NIS in nationales Recht

12/2020
Vorstellung der EU-Cybersicherheitsstrategie durch Europäische Kommission

04/2021
Erster Vorschlag für NIS2-Richtlinie durch Europäische Kommission

12/2022
Genehmigung der NIS2-Richtlinie durch die einzelnen EU-Organe

01/2023
NIS2-Richtlinie tritt in Kraft

10/2024
Frist für Umsetzung der NIS2 in nationales Recht

Wer ist betroffen?

Im Gegensatz zur ursprünglichen NIS zieht die NIS2 keine Trennlinie mehr zwischen Betreibern wesentlicher Dienste und Anbietern digitaler Dienste. Stattdessen werden Einrichtungen nach ihrer Wichtigkeit in zwei Kategorien eingeordnet: wesentliche und wichtige Einrichtungen, die jeweils unterschiedlichen Aufsichtsregelungen unterworfen sind.

Demnach sind alle Sektoren und Organisationen, die in der NIS2 gelistet werden, von großer Bedeutung für die Mitglieder der Europäischen Union. Man geht davon aus, dass es der Gesellschaft schweren Schaden zufügen würde, wenn diese durch Störungen nicht mehr in der Lage wären, ihre Aufgaben zu erfüllen. Letztlich trägt die Unterscheidung in die zwei Kategorien dem Fakt Rechnung, dass ein Sicherheitsvorfall nicht in allen Sektoren die gleichen Auswirkungen auf die Gesellschaft nach sich ziehen würde.

Betroffene Branchen

Wesentliche Einrichtungen (Essential Entities, EE)

Große Organisationen in Sektoren mit **hoher Kritikalität** sowie Sonderfälle.

Definition große Organisationen

> 250 Mitarbeiter
> 50 Millionen Euro Umsatz
> 43 Millionen Euro Bilanzsumme

Sektoren mit hoher Kritikalität

- Energie
- Verkehr
- Bankwesen
- Verwaltung von IKT-Diensten
- Trinkwasser
- Abwasser
- Gesundheitswesen
- Digitale Infrastruktur
- Öffentliche Verwaltung
- Finanzmarktinfrastruktur
- Weltraum

Wichtige Einrichtungen (Important Entities, IE)

Große Organisationen sonstig. kritischer Sektoren und **mittlere Unternehmen.**

Definition mittlere Unternehmen

50 - 250 Mitarbeiter
10 - 50 Millionen Euro Umsatz
< 43 Millionen Euro Bilanzsumme

Sonstige kritische Sektoren

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

Beide Arten von Einrichtungen haben nach der NIS2 grundsätzlich dieselben Aufgaben und Pflichten. So müssen beispielsweise die Mitglieder der Leitungsorgane wesentlicher und wichtiger Einrichtungen an Schulungen teilnehmen sowie geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen zu ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme zu beherrschen .

Einrichtungen sollen diese für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen, um die Auswirkungen von Sicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Dienste zu verhindern oder möglichst gering zu halten.

Wesentliche Organisationen werden zudem verpflichtet, proaktiv wirkende Maßnahmen zu implementieren, mit denen die Auswirkungen von Missmanagement auch dann erkannt werden können, wenn kein konkreter Sicherheitsvorfall vorliegt.

Wichtige Einrichtungen hingegen werden aufgefordert, die Richtlinie „reaktiv" umzusetzen. Die Einhaltung der entsprechenden Gesetze und Vorgaben ist verpflichtend, wird aber nur geprüft, wenn ein tatsächlicher Vorfall vorliegt.

Wird bei einer solchen Prüfung festgestellt, dass die Maßnahmen der Organisation nicht den Vorgaben entsprachen, sind sowohl für wesentliche als auch für wichtige Einrichtungen Bußgelder und andere Strafen möglich.

Im diesem Zusammenhang ist anzumerken, dass die jeweils verantwortlichen Behörden verpflichtet sind, der Kommission sowie der Kooperationsgruppe bis zum 17. April 2025 und danach jeweils für zwei Jahre die Anzahl wesentlicher und wichtiger Einrichtungen für jeden Sektor im eigenen Land mitzuteilen.

Sorgfalts- und Berichtspflichten

Alle Organisationen, die in der NIS2 benannt werden – egal, ob wesentlich oder wichtig – werden verpflichtet, bestimmte Sorgfaltspflichten zu erfüllen. Die Richtlinie listet eine Reihe von Maßnahmen, die Anbieter von Diensten mindestens durchführen müssen.

Dazu gehören Risikobewertungen um sicherzustellen, dass die Organisation der Sicherheit der Informationssysteme genügend Aufmerksamkeit zukommen lässt, ein Krisenmanagement, Maßnahmen zur Aufrechterhaltung des Betriebs im Fall eines größeren Cybersicherheits-Vorfalls sowie Maßnahmen für die Sicherheit in der Lieferkette. Zusätzlich gehören zu den Sorgfaltspflichten die Absicherung von Netzwerk- und Informationssystemen mithilfe von Kryptographie und Verschlüsselung sowie die Einführung von Richtlinien und Prozessen, um die Wirksamkeit der Risikomanagements zu prüfen.

Auch die Berichtspflichten gelten für alle Einrichtungen, die die NIS2 benennt. Diese Berichtspflichten fordern die entsprechenden Organisationen auf, im Fall eines Sicherheitsvorfalls die zuständigen nationalen Behörden innerhalb von 24 Stunden darüber zu informieren. 72 Stunden später sind weitere Informationen zum Vorfall zu melden, einen Monat nach dem Vorfall muss ein Abschlussbericht eingereicht werden.

Sorgfaltspflichten

In der ursprünglichen NIS-Richtlinie galten die Sorgfaltspflichten sowohl für Anbieter wesentlicher Dienste als auch für Anbieter digitaler Dienste. Zu den Pflichten gehörte es, angemessene und verhältnismäßige technische und organisatorische Maßnahmen zu ergreifen, um mit Risiken für die Sicherheit von Netzwerk- und Informationssystemen umzugehen.

Die neue NIS2 hingegen unterscheidet nun zwischen wesentlichen und wichtigen Einrichtungen. Diese Unterscheidung beruht einerseits auf der Kritikalität des Sektors, zu dem die Einrichtung gezählt wird, andererseits auf der Art des Dienstes, den sie bereitstellt sowie ihrer Größe.

Sowohl wesentliche als auch wichtige Einrichtungen werden verpflichtet, die Sorgfaltspflichten zu erfüllen. Es liegt jedoch in der Hand der Mitgliedsstaaten selbst, welche Einrichtungen zu wesentlichen und welche zu den wichtigen Einrichtungen gezählt werden sollen. Grundlage der Einteilung sollen die am besten angemessenen nationalen Mechanismen sein, die es den Einrichtungen ermöglichen, sich selbst einer Kategorie zuzuordnen.

Die Einrichtungen sind zu Maßnahmen des Cybersicherheits-Risikomanagements verpflichtet, wenn sie einer der beiden Kategorien zugeordnet sind. Diese sollten in einem angemessenen Verhältnis zum Grad der Risikoexposition der wesentlichen oder wichtigen Einrichtung stehen und den gesellschaftlichen und wirtschaftlichen Auswirkungen Rechnung tragen, die ein Sicherheitsvorfall haben würde. Zusätzlich ist die Kritikalität, die Größe der Organisation und die Wahrscheinlichkeit des Auftretens von Vorfällen zu berücksichtigen.

In diesem Kontext meint die „Sicherheit" von Netzwerk- und Informationssystemen deren Resilienz gegenüber Aktivitäten, die die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit der verarbeiteten Daten beeinträchtigen könnten. Die Durchführungsverordnung (EU) 2018/151 der Kommission legt zusätzlich fest, welche Elemente der Cybersicherheit zu betrachten sind: Sicherheit von Systemen und Anlagen, Bewältigung von Sicherheitsvorfällen, Betriebskontinuitätsmanagement (Business continuity management), Überwachung, Überprüfung und Erprobung und internationale Normen.

In der NIS2-Richtlinie wird eine Reihe von Maßnahmen gelistet, die mindestens zu implementieren sind, darunter die Durchführung einer Risikoanalyse und das Aufstellen von Richtlinien für die Sicherheit von Informationssystemen, die Behandlung von Sicherheitsvorfällen, das Betriebskontinuitäts- und Krisenmanagement, die Absicherung von Lieferketten und für die Beschaffung, Entwicklung und Wartung von Netzwerk- und Informationssystemen. Auch Vorgaben und Prozesse, mit denen die Wirksamkeit des Risikomanagements bewertet werden kann, und der Einsatz von Kryptographie und Verschlüsselung sind Teil der NIS2-Richtlinie.

Wesentliche und wichtige Einrichtungen werden außerdem aufgefordert, einige Praktiken der Cyberhygiene anzuwenden, also z.B. Zero-Trust-Grundsätze, Software-Updates, Gerätekonfiguration, Netzwerksegmentierung, Identitäts- und Zugriffsmanagement oder Mechanismen zur Sensibilisierung der Nutzer zu implementieren, Schulungen für ihre Mitarbeiter zu organisieren und das Bewusstsein für Cyberbedrohungen, Phishing oder Social-Engineering-Techniken zu schärfen.

Zusätzlich sind die Organisationen aufgefordert, ihre eigenen Cybersicherheitskapazitäten neu zu bewerten und gegebenenfalls die Integration von Technologien zur Verbesserung der Cybersicherheit voranzutreiben. Hierzu gehört beispielsweise der Einsatz künstlicher Intelligenz oder von Systemen maschinellen Lernens, um die Kapazitäten und die Sicherheit der eigenen Netz- und Informationssysteme zu erhöhen.

Um die Einhaltung der neuen Regeln sicherzustellen, dürfen die einzelnen Mitgliedsstaaten wesentliche und wichtige Einrichtungen auffordern, bestimmte IT-Produkte, -Dienste oder Prozesse zu nutzen, die entsprechend den Vorgaben des EU-Rechtsakt zur Cybersicherheit **(EU) 2019/881)** zertifiziert sein müssen

Weiterhin steht es der Europäischen Kommission frei, Durchführungs- und weitere Rechtsakte zu erlassen, um die geforderten Risikomanagementmaßnahmen weiter zu spezifizieren. So lassen sich die Vorgaben der Richtlinie vor dem Hintergrund neuer Cyber-Bedrohungen, technologischer Entwicklungen oder sektorspezifischer Merkmale bei Bedarf anpassen.

Berichtspflichten

In der NIS2-Richtlinie werden zusätzlich zu den genannten Sorgfaltspflichten Berichtspflichten erweitert und konkretisiert, die bereits in der ursprünglichen NIS erwähnt worden waren.

Mit der ersten NIS-Richtlinie hatte man die Verpflichtung eingeführt, Sicherheitsvorfälle zu melden, wenn diese die Verfügbarkeit der Dienste beeinträchtigten. Der Richtlinie zufolge handelt es sich um einen Sicherheitsvorfall, wenn das Ereignis „tatsächlich nachteilige Auswirkungen auf die Sicherheit von Netz- und Informationssystemen“ hat. „Sicherheit“ meint die hier die „Fähigkeit von Netz- und Informationssystemen, alle Angriffe abzuwehren, die die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter oder übermittelter oder verarbeiteter Daten oder entsprechender Dienste, die über diese Netz- und Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigen.“

Verschiedene Parameter sollen helfen festzustellen, ob sich ein Sicherheitsvorfall in erheblichem Maße auf die bereitgestellten Dienste auswirkt, darunter die Zahl betroffener Nutzer, die Dauer des Vorfalls sowie die geografische Ausbreitung des Gebiets, das von einem Sicherheitsvorfall betroffen sein könnte. Könnte sich ein Sicherheitsvorfall für einen Anbieter in erheblichem Maße auf die bereitgestellten Dienste auswirken, hat dieser ihn unverzüglich an das örtliche Computer Security Incident Response Team (CSIRT) oder die durch das Mitgliedsland festgelegte zuständige Behörde zu melden. Der Bericht muss ausreichend Informationen enthalten, sodass

Berichtspflichten: Ablauf nach NIS2

24 Stunden nach Kenntnisnahme des Sicherheitsvorfalls (und unverzüglich) ist eine erste Meldung an die zuständige Behörde oder das für das entsprechende Mitgliedsland zuständige CSIRT zu machen. Dabei soll wenn möglich angegeben werden, ob der Verdacht besteht, dass der erhebliche Sicherheitsvorfall auf rechtswidrige oder böswillige Handlungen zurückzuführen ist. Hiermit sind die unbedingt notwendigen Informationen abgedeckt

Innerhalb von 72 Stunden nach der ersten Meldung muss die betroffene Einrichtung eine Aktualisierung und eine erste Bewertung mit genaueren Angaben zum Angriff und den getroffenen Maßnahmen vorlegen. Auf Wunsch der Einrichtung kann sie Informationen zu möglichen Gegenmaßnahmen erhalten und, falls nötig, zusätzliche technische Unterstützung anfordern. Geht der Angriff auf eine rechtswidrige Handlung zurück, erhält die betroffene Einrichtung außerdem Hinweise zur Meldung des Vorfalls an die Strafverfolgungsbehörden.

Innerhalb eines Monats nach Einreichung der ersten Meldung ist ein Abschlussbericht vorzulegen. Dieser muss Folgendes enthalten:

- eine detaillierte Beschreibung des Vorfalls, seines Schweregrads und seiner Folgen
- die Art der Bedrohung oder die Ursache, die dem Vorfall vermutlich zugrunde liegt
- durchgeführte und laufende Gegenmaßnahmen

die zuständige Behörde oder das CSIRT die grenzüberschreitenden Auswirkungen des Vorfalls evaluieren können.

Die NIS2-Richtlinie wiederum unterteilt die Berichtspflichten in zwei Stufen. Die erste Meldung dient dazu, die mögliche Ausbreitung des Sicherheitsvorfalls zu vermeiden und Einrichtungen die Möglichkeit zu geben, Unterstützung einzuholen. Die zweite Meldung soll umfangreicher und detaillierter sein und sicherstellen, dass Lehren aus vergangenen Sicherheitsvorfällen gezogen werden können.

Hier werden allerdings vermutlich weitere Klarstellungen vonseiten der nationalen Gesetzgeber nötig sein, um jeden Vorfall und seine Folgen eindeutig bewerten zu können. Die Berichtspflichten der NIS2 sollen weiterhin helfen, die Widerstandsfähigkeit einzelner Unternehmen und ganzer Sektoren gegenüber Cyber-Bedrohungen zu stärken.

Die Bestimmung über die Meldung von Vorfällen mit erheblichen Folgen wurde aus der NIS in die NIS2-Richtlinie übernommen. Hinzugefügt wurde, dass die Einrichtungen nun auch jede von ihnen festgestellte größere Cyber-Bedrohung melden müssen, die zu einem erheblichen Vorfall hätte führen können. Die Definition des Begriffs „Cybersicherheit“ wiederum folgt der Definition in der Verordnung über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik (EU) 2019/881, dem EU-Cybersicherheitsgesetz.

Hierin wird Cybersicherheit definiert als „alle Tätigkeiten, die notwendig sind, um Netz- und Informationssysteme, die Nutzer solcher Systeme und andere von Cyberbedrohungen betroffene Personen zu schützen." Ein Sicherheitsvorfall gilt als signifikant, wenn er zu einer erheblichen Störung des Betriebs oder finanziellen Verlusten für die betroffene Einrichtung geführt hat oder hätte führen könnte oder wenn der Vorfall erhebliche materielle oder immaterielle Schäden verursacht und so natürliche oder juristische Personen beeinträchtigt hat oder beeinträchtigen kann.

Einrichtungen, die nicht unter die NIS2-Richtlinie fallen, können trotzdem freiwillig signifikante Sicherheitsvorfälle, Cyber-Bedrohungen oder Beinahe-Vorfälle melden. Die zuständige Behörde oder CSIRT verarbeitet die Meldung entsprechend dem „Zwei-Stufen"-Berichtsprozedere.

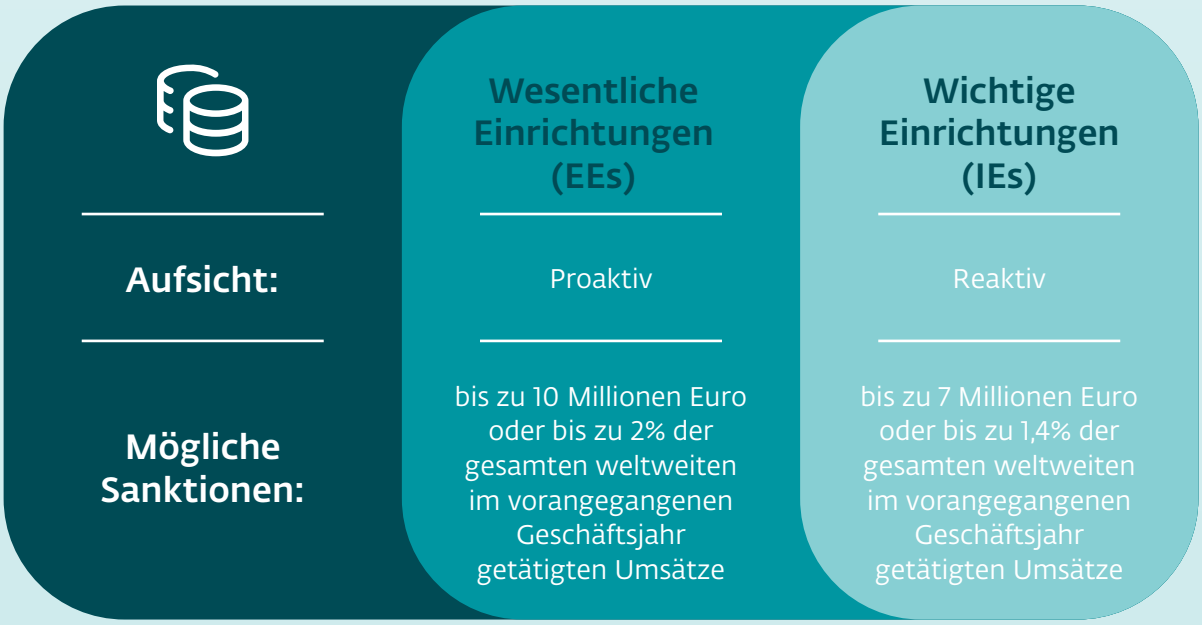
Freiwillig eingereichte Meldungen ziehen keine weiteren Verpflichtungen nach sich. Meldet ein Unternehmen also freiwillig einen (Beinahe-)Vorfall oder eine Bedrohung, sollen ihm daraus nicht mehr Verpflichtungen erwachsen, als wenn es die Meldung nicht abgegeben hätte.

Umsetzung der NIS2

Es obliegt den Mitgliedstaaten, Kontrollmechanismen einzuführen, die die Einhaltung der Anforderungen der NIS2 sicherstellen, sobald sie diese in nationales Recht umgesetzt haben.

Für wesentliche Organisationen ergibt sich eine Verpflichtung zu proaktiver Aufsicht und Kontrolle. Im Gegensatz dazu ergibt sich für die wichtigen Organisationen lediglich eine reaktive Aufsichtsverpflichtung, die durch konkrete Belege, Hinweise oder Informationen darüber angestoßen werden, dass die jeweilige Einrichtung den Pflichten der Richtlinie nicht nachkommt.

Tatsächlich sollen die zuständigen Behörden im zweiten Fall nur dann aktiv werden, wenn einem Mitgliedstaat der Eindruck erwächst, dass eine wichtige Einrichtung die Vorgaben der Richtlinie nicht befolgt.



Für eine Definition wesentlicher und wichtiger Einrichtungen siehe Tabelle auf Seite 5.

Die Durchsetzungsmaßnahmen der zuständigen Behörden sollen wirksam, angemessen und abschreckend sein. Sowohl für wesentliche als auch für wichtige Einrichtungen sind die entsprechenden Behörden berechtigt, Vor-Ort-Kontrollen und externe nachträgliche Aufsichtsmaßnahmen, durch geschulte Fachkräfte durchführen zu lassen.

Möglich sind außerdem gezielte Sicherheitsprüfungen, Sicherheitsscans, die Anforderung von Daten, Dokumenten und Informationen sowie die Anforderung von Nachweisen für die Umsetzung der Cybersicherheitskonzepte. Dazu gehören beispielsweise Ergebnisse der von einem qualifizierten Prüfer durchgeführten Sicherheitsprüfungen und die entsprechenden zugrunde liegenden Nachweise.

Für wesentliche Einrichtungen können zudem Stichprobenkontrollen und Ad-hoc-Prüfungen durchgeführt werden. Außer in hinreichend begründeten Fällen tragen die Kosten für die Sicherheitsprüfungen die geprüften Einrichtungen.

Wird ein Verstoß erkannt, haben die zuständigen Behörden weitere Durchsetzungsrechte. So können sie Warnungen aussprechen, verbindliche Anweisungen erlassen oder die betreffenden Einrichtungen anweisen, das gegen diese Richtlinie verstoßende Verhalten einzustellen.

Außerdem können sie die betreffenden Einrichtungen anweisen, diejenigen natürlichen oder juristischen Personen, die potenziell vom Verstoß betroffen sind, zu informieren, oder sogar fordern, dass die Information darüber öffentlich bekannt gemacht werden.

Sollten diese Maßnahmen nicht zur Verbesserung der Lage ausreichen, können die zuständigen Behörden die Aktivitäten der Einrichtung vorübergehend aussetzen oder den Personen auf Leitungsebene vorübergehend untersagen, Leitungsaufgaben als Geschäftsführer oder als rechtliche Vertretung des Unternehmens wahrzunehmen.

Mit einer Liste möglicher Sanktionen, die die Behörden bei Verstößen gegen die Vorgaben für Risikomanagement und Berichtspflichten verhängen können, schafft die NIS2-Richtlinie einen einheitlichen Sanktionsrahmen innerhalb der EU.

Zu den möglichen Sanktionen gehören verbindliche Anweisungen, die Anweisung zur Umsetzung von im Rahmen einer Sicherheitsprüfung formulierten Empfehlungen, die Anweisung zur Anpassung der Sicherheitsmaßnahmen an die Vorgaben der NIS2 sowie das Verhängen von Bußgeldern.

Die Mitgliedsstaaten sind verpflichtet, die entsprechenden Behörden zu ermächtigen, hohe Geldstrafen zu verhängen. Für wesentliche Einrichtungen sind mindestens 10.000.000 Euro oder 2% der gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsätze anzusetzen – je nachdem, welcher Betrag höher ist. Für wichtige Einrichtungen wurde der Höchstbetrag auf 7.000.000 Euro bzw. 1,4% der gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsätze gesetzt. Auch hier gilt wieder der Betrag, der höher ausfällt.

Die Leitungsorgane wesentlicher und wichtiger Einrichtungen können für die Nichteinhaltung der NIS2-Richtlinie haftbar gemacht werden. Handelt es sich bei Ihrer Organisation um eine der Einrichtungen, die in der Richtlinie aufgeführt sind und versäumt sie es, eine unternehmensweite Cyber-Resilienz aufzubauen und aufrechtzuerhalten, sind Strafzahlungen und Sanktionen für die Nichteinhaltung von Pflichten des Risikomanagements oder Berichtspflichten die Folge.

Zur Stärkung der Aufsichtsbefugnisse und der Maßnahmen, die zu einer wirksamen Befolgung der Vorschriften beitragen, gibt die NIS2-Richtlinie einen Mindestumfang an Aufsichtsmaßnahmen und -mitteln vor, mit welchen die zuständigen Behörden wesentliche und wichtige Einrichtungen prüfen und beaufsichtigen können.

Hierzu gehören regelmäßige und gezielte Sicherheitsprüfungen, Vor-Ort-Kontrollen und externe Aufsichtsmaßnahmen, die Anforderung von Informationen oder Zugang zu Dokumenten und Nachweisen.

Bei der Ergreifung von Durchsetzungsmaßnahmen müssen die zuständigen Behörden den Umständen des Einzelfalls Rechnung tragen, beispielsweise der Art, Schwere und Dauer des Verstoßes, dem verursachten Schaden oder den verursachten Verlusten sowie dem etwaigem Vorliegen von Vorsatz oder Fahrlässigkeit.

Um die Verantwortlichkeit für die Cybersicherheit auf organisatorischer Ebene zu gewährleisten, enthält die NIS2 Vorgaben zur Haftung natürlicher Personen in Leitungspositionen in Einrichtungen, die unter die neue Richtlinie fallen.

Was bedeutet die NIS2 für kleine und mittelständische Unternehmen?

Die NIS2 legt fest, dass bestimmte Kriterien für die Unternehmensgröße anzulegen sind – nachzulesen auch in der Tabelle auf Seite 5 . Dadurch ist die Mehrheit der kleinen und mittleren Unternehmen nicht von den Bestimmungen der Richtlinie betroffen.

Es gibt jedoch Ausnahmen. KMU in den Sektoren elektronischer Kommunikationsnetze oder öffentlich zugänglicher elektronischer Kommunikationsdienste, Vertrauensdiensteanbieter und TLD (Top Level Domain)-Namenregister fallen unabhängig von ihrer Größe unter die neuen Regelungen.

Kleine und mittlere Unternehmen werden immer häufiger zum Ziel von Angriffen auf die Lieferkette. Grund sind vor allem begrenzte Ressourcen für die Absicherung der Unternehmenssysteme.

Ein solcher Angriff auf die Lieferkette kann Folgen für alle Einrichtungen haben, für die sie Güter oder Dienste bereitstellt. Die Mitgliedsstaaten der EU sind daher gut beraten, KMU dabei zu unterstützen, Herausforderungen innerhalb der Lieferkette zu bewältigen, beispielsweise durch nationale Strategien für die Cybersicherheit.

Auf nationaler und regionaler Ebene sollten Anlaufstellen für kleine und mittelständische Unternehmen geschaffen werden, die diese entweder direkt beraten und unterstützen oder sie an die entsprechenden Stellen verweisen, an denen sie Beratung und Unterstützung bei Fragen zur Cybersicherheit bekommen können.

In einer Stellungnahme im März letzten Jahres begrüßte die Europäische Allianz digitaler KMU DIGITAL SME, das größte Netzwerk kleiner und mittlerer IKT-Unternehmen in der EU, den Vorschlag zur NIS2. Gleichzeitig warnten die Experten vor den indirekten Folgen der Richtlinie für KMU.

James Philpot, Project Manager bei DIGITAL SME zufolge sollten Unternehmen sich zunächst beim Cybersicherheits-Zentrum ihres jeweiligen Landes informieren und die Leitfäden und Empfehlungen der ENISA konsultieren.

So könnten sie in Erfahrung bringen, wie die spezifischen Anforderungen zur Stärkung der unternehmenseigenen Cybersicherheit aussehen. Dabei sei es aber nicht für alle gleich einfach oder schwierig, die passenden Informationen zu erhalten, da die verschiedenen EU-Mitgliedsstaaten sehr unterschiedliche Ressourcen zur Verfügung stellen.

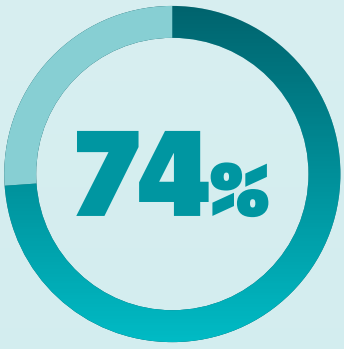
Nichtsdestotrotz verpflichte die NIS2 die EU-Mitglieder, Unterstützung und Ressourcen bereitzustellen, insbesondere wenn es darum geht, die Richtlinie und ihren Anwendungsbereich zu verstehen. Dies wiederum helfe den Unternehmen zu erkennen, ob ihre Kunden unter die Regelungen fallen und entsprechend gezielter zu agieren.

„In Zukunft werden vor allem nachgelagerte Zulieferer von Angriffen und Vorfällen betroffen sein und häufig besitzen sie nicht die technischen Ressourcen, die es dann eigentlich bräuchte. Schon im ersten Schritt ist es für sie jedoch schwierig, die Berichtspflichten nachzuvollziehen und zu durchdringen, wie die NIS2 mit der bestehenden Gesetzgebung zusammenhängt," erklärt Philpot.

KMU: Vertrauen in die eigene Cyberabwehr

Nur 48% aller kleinen und mittelständischen Unternehmen geben an, mittleres bis großes Vertrauen in die eigene Cyberabwehr zu haben.

7%	kein Vertrauen
10%	hohes Vertrauen
38%	mittleres Vertrauen
45%	geringes Vertrauen



74% aller KMU halten sich aufgrund ihrer Größe für anfälliger für Cyberangriffe als Großunternehmen und Konzern.

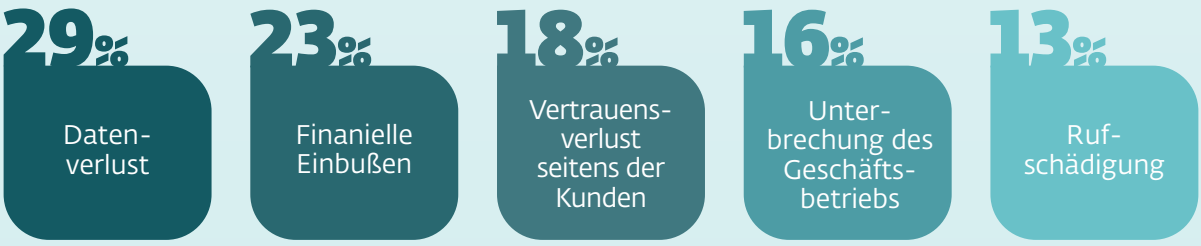
Quelle: ESET Cybersicherheits-Umfrage bei KMU (2022)

Grundsätzlich sind alle Bestrebungen, das Niveau der Cybersicherheit bei EU-Unternehmen zu erhöhen, begrüßenswert. Außerdem, so sind sich DIGITAL SME und ESET sicher, könnte der neue gesetzliche Rahmen vielversprechende Chancen bereithalten. Allerdings macht Philpot auch deutlich, dass letztlich die Umsetzung und die Unterstützung der Unternehmen durch die Behörden darüber entscheiden werden, ob die neue Richtlinie zur großen Hilfe für die Unternehmen wird oder sie schlichtweg überlastet.

Auf dem europäischen Markt gibt es eine Vielzahl von Anbietern, die Unternehmen helfen, das geforderte Cybersicherheitsniveau zu erreichen. Hier gilt es jedoch, nicht blind den bekanntesten Anbieter oder das günstigste Angebot zu wählen, da diese nicht selten nicht aus der EU kommen. Stattdessen ist es wichtig, die Unterstützung durch die Behörden und die unternehmenseigenen Ressourcen zusammenzudenken, um die Richtlinie optimal zu nutzen und die Innovationskraft Europas zu stärken.

Kleine und mittelständische Unternehmen haben außerdem die Möglichkeit, sich an ihre nationalen CSIRTs zu wenden, um die Umsetzung der NIS2 auf nationaler Ebene zu verbessern. Auch Ressourcen wie der Leitfaden der DIGITAL SME (SBS Guide) sowie der Leitfaden DIGITAL SME Guide on Information Security Controls oder Zertifizierungen der unternehmenseigenen Cybersicherheit können sehr hilfreich sein.

Die größten Sorgen für KMU in Bezug auf Cyberangriffe und ihre Folgen



Quelle: ESET Cybersicherheits-Umfrage bei KMU (2022)

Wie Philpot im Gespräch mit ESET feststellt, wissen die KMU nur zu gut um die möglichen Folgen von Cyberattacken: Datenverluste, finanzielle Einbußen und der Verlust des Vertrauens seitens der Kunden. Hier kann die NIS2 eine große Chance darstellen, indem sie hilft, die Security Awareness innerhalb des Unternehmens zu stärken und die unternehmenseigene Cyber-Resilienz zu erhöhen.

In ESETs Digital Security Guide finden Sie laufend hilfreiche Tipps für Ihre IT-Security als kleines oder mittelständisches Unternehmen.

Digital Security
Progress. Protected.

Seit mehr als 30 Jahren ist ESET® ein weltweit führender Hersteller von IT-Security. Unsere Software und weitere Dienstleistungen schützen Unternehmen, Kritische Infrastrukturen und Heimanwender vor immer neuen digitalen Bedrohungen. Neben Endpoint und Mobile Security bietet ESET Lösungen für EDR (Endpoint Detection and Response) ebenso wie Verschlüsselungs- und Authentifizierungslösungen. Die leistungsstarken, nutzerfreundlichen Lösungen schützen rund um die Uhr, ohne laufende Prozesse zu behindern und sorgen dafür, dass Nutzer rundum sicher sind und Unternehmensabläufe jederzeit ungehindert weiterlaufen können.

Die stetige Weiterentwicklung der Bedrohungslandschaft fordert einen Security-Anbieter, der die Nutzung von Technologie einfach sicher macht. Dank Forschungs- und Entwicklungsabteilungen überall auf der Welt sorgen wir laufend für eine sicherere Zukunft für alle. Weitere Informationen finden Sie auf www.eset.de oder folgen Sie uns.

welivesecurity by ESET

EVERSHEDS SUTHERLAND

Eversheds Sutherland ist eine weltweit agierende Anwalts- und Notariatskanzlei mit 74 Büros in 35 Ländern und mehr als 3.000 Anwälten. Dank unserer internationalen Ausrichtung sind wir wie keine andere Kanzlei in der Lage, grenzüberschreitend zu beraten. In Europa hat Eversheds Sutherland 44 Niederlassungen.

Diese Übersicht wurde in Zusammenarbeit mit ESET Government Affairs erstellt.

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

ESET.DE | ESET.AT | ESET.CH