WHITEPAPER

Cybersecurity und die neue Rechtslage

Alles, was Sie über die NIS2-Richtlinie wissen müssen

ESET 100% Made in EU IT-Security

EVERSHEDS SUTHERLAND & ESET Digital Security Progress. Protected.

ESET.DE/NIS2

Digital Security
Progress. Protected.

Einleitung

Wir freuen uns, dass Sie sich für unser Whitepaper zur NIS2-Richtlinie interessieren. Darin werden wir die wichtigsten Aspekte der NIS2-Richtlinie vorstellen und verdeutlichen, in welchem Ausmaß sie für Unternehmen in der EU gilt.

Die NIS2-Richtlinie ist die überarbeitete Version der in 2016 eingeführten Richtlinie zur Sicherheit von Netz- und Informationssystemen (NIS) mit dem Ziel, die Cybersicherheit in der Europäischen Union (EU) noch mehr zu stärken. Sie soll Unternehmen helfen, sich vor Cyberbedrohungen zu schützen und die digitale Infrastruktur der EU sicherer und widerstandsfähiger zu machen. Nach der offiziellen Veröffentlichung der Richtlinie haben die Mitgliedstaaten nun 21 Monate Zeit - das heißt konkret, bis zum 17. Oktober 2024 - um ihre Vorgaben in deren nationale Gesetzgebung zu integrieren und in die Praxis umzusetzen.

In diesem Whitepaper geben unsere Experten einen Überblick über die wichtigsten Anforderungen der NIS2-Richtlinie und in welchem Umfang sie für Unternehmen in der EU gelten. Auch die damit verbundenen Verpflichtungen zur Einhaltung der Vorgaben werden hierin beleuchtet.

Mithilfe dieses Whitepapers erfahren Sie, wie Sie Ihr Unternehmen vor Cyber-Bedrohungen schützen können und die NIS2-Richtlinie problemlos einhalten.

ESET.DE/NIS2

Inhaltsverzeichnis

1. **Welche Bedeutung** hat die NIS2-Richtlinie?

Ist Ihr Unternehmen mittelgroß oder groß und in einem der kritischen Sektoren wie Energie, Verkehr, Gesundheit und digitale Infrastruktur angesiedelt? In dem Fall ist es mehr als wahrscheinlich, dass die neue EU-Gesetzgebung große Auswirkungen auf die Cybersicherheit in Ihrem Unternehmen haben wird. "Diese europäische Richtlinie wird rund 160.000 Unternehmen helfen, ihre IT-Sicherheit zu verbessern und Europa zu einem sicheren Ort zum Leben und Arbeiten zu machen. Die Richtlinie hat zum Ziel, den Austausch von Informationen mit dem privaten Sektor und Partnern in der ganzen Welt zu ermöglichen. Wenn wir im professionellen Stil angegriffen werden, müssen wir auch im professionellen Stil reagieren", erklärt der niederländische Europaabgeordnete Bart Groothuis.

Angesichts des extrem hohen Stellenwerts von Cybersicherheit für den Schutz unserer Gesellschaft hat die Europäische Union 2016 die erste Richtlinie zur Netz- und Informationssicherheit (NIS-Richtlinie) eingeführt. Auch wenn sie für mehr Kohärenz innerhalb der EU im Bereich der Informationssicherheit gesorgt hat, muss die Cyber-Resilienz in den Augen des Europäischen Parlaments noch weiter erhöht werden, um in Zukunft einen wirksamen Schutz zu bieten. Angesichts der zunehmenden Digitalisierung und der großen Anzahl an Cyberangriffen wurde die NIS-Richtlinie überarbeitet und verbessert. Die NIS2-Richtlinie wird eine größere Reichweite haben und sich auf weit mehr Sektoren erstrecken, mit dem Ziel, so noch umfassender die Cyber-Resilienz von EU ansässigen Unternehmen zu stärken.

> *Diese europäische Richtlinie wird rund 160.000 Unternehmen dabei helfen, ihre Sicherheit zu verbessern und Europa zu einem sicheren Ort zum Leben und Arbeiten zu machen.*
>
> *Bart Groothuis,*
> *niederländischer Europaabgeordneter*

Risikomanagement und Zusammenarbeit

Doch wie genau wird diese überarbeitete Richtlinie eine bessere Cyber-Resilienz gewährleisten? Die NIS2-Richtlinie ist darauf ausgerichtet, das Niveau der Cybersicherheit auf verschiedene Weisen anzuheben und zu synchronisieren. Sie verschärft die auferlegten Schutzanforderungen, konzentriert sich auf die Sicherheit der Lieferkette (Produktionsketten eingeschlossen), zieht die Meldepflichten an, verschärft die Aufsichtsmaßnahmen und führt Durchsetzungsauflagen mit vereinheitlichten Strafmaßnahmen in allen Mitgliedstaaten ein. Die Bedeutung des Informationsaustauschs und der (inter)nationalen Zusammenarbeit im Bereich des Krisenmanagements ist ebenfalls ein Punkt auf der Agenda.

Der Anwendungsbereich der NIS2-Richtlinie

Die NIS2-Richtlinie erstreckt sich über mehr Sektoren als die ursprüngliche NIS-Richtlinie. In der ersten wurden nur die Bereiche Gesundheitswesen, Verkehr, Banken und Finanzmarktinfrastruktur, digitale Infrastruktur, Wasserversorgung, Energie und Anbieter digitaler Dienste genannt. Dabei konnten die Mitgliedstaaten festlegen, welche Organisationen als wesentlich angesehen wurden. Mit der NIS2-Richtlinie werden einheitliche Regeln für mittlere sowie große Unternehmen eingeführt, die in kritischen Sektoren wie Energie, Verkehr, Gesundheit und digitale Infrastruktur tätig sind. Dazu gehören nun "Sektoren mit hoher Kritikalität" wie Energie, Verkehr, Banken, Finanzmarktinfrastruktur, Gesundheitswesen, Trinkwasser, Abwasser, digitale Infrastruktur, IKT-Management (B2B), Regierung und Raumfahrt sowie "sonstige kritische Sektoren" wie Post- und Kurierdienste, Abfallwirtschaft, Chemie, Lebensmittel, verarbeitendes Gewerbe, digitale Anbieter und Forschung. Alle mittleren und großen Unternehmen in diesen Sektoren werden von den Rechtsvorschriften erfasst.

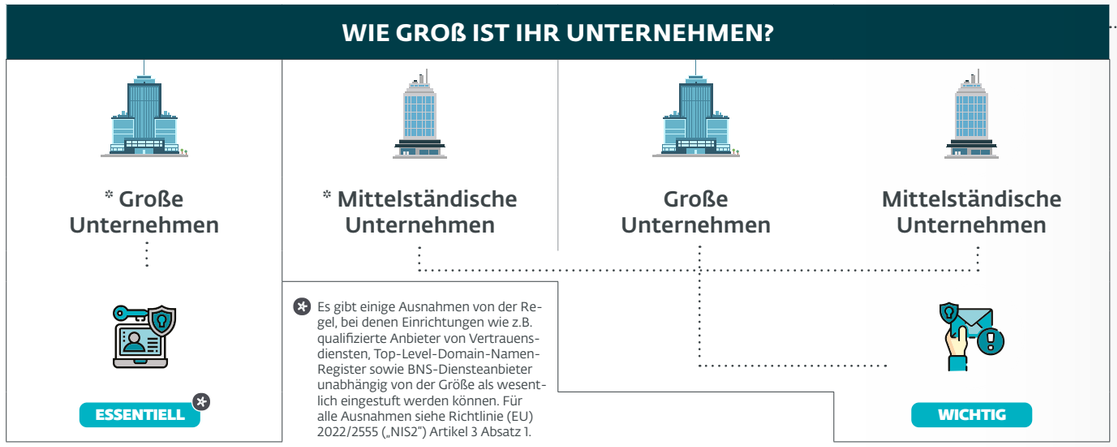
2. Fällt Ihr Unternehmen in die Kategorien wesentlich oder wichtig?

Die Art und Weise, wie die Durchsetzung erfolgt, hängt davon ab, in welche Kategorie ein Unternehmen fällt. Im Rahmen der NIS2-Richtlinie gibt es zwei Kategorien: Unternehmen können als wesentlich oder als wichtig eingestuft werden. Ob eine Einordnung als wesentlich oder wichtig erfolgt, hängt davon ab, ob das Unternehmen in einen kritischen oder sehr kritischen Sektor fällt und von der jeweiligen Größe.

Mittelständische Unternehmen mit weniger als 250 Beschäftigten und einem Jahresumsatz von bis zu 50 Millionen Euro (oder einer Bilanzsumme von bis zu 43 Millionen Euro), die in sehr kritischen Sektoren tätig sind, gelten als wichtig, ebenso wie andere große und mittlere Unternehmen in kritischen Sektoren. Nur große Unternehmen, die die Schwellenwerte für mittelständische Unternehmen überschreiten und in sehr kritischen Sektoren tätig sind, gelten als wesentlich. Einige Unternehmen werden unabhängig von ihrer Größe automatisch als "wesentlich" eingestuft, wenn ein Ausfall der Dienste schwerwiegende Folgen für die Gesellschaft hätte oder sie der einzige nationale Anbieter sind. Dazu gehören Unternehmen, die öffentliche Kommunikationsnetze und -dienste bereitstellen, Anbieter von Vertrauensdiensten sowie Anbieter von Top-Level-Domain-Namen und Domain-Namen-Registrierungsdiensten.

Grundsätzlich zielt die NIS2-Richtlinie nicht auf Klein- und Kleinstunternehmen ab, die weniger als 50 Mitarbeiter und einen Jahresumsatz von weniger als 7 Millionen Euro (oder eine Bilanzsumme von weniger als 5 Millionen Euro) haben. Spielen sie allerdings eine Schlüsselrolle für die Gesellschaft, Wirtschaft, Sektoren oder Dienstleistungen, sind die Mitgliedstaaten verantwortlich, sie in dieser Richtlinie zu erfassen.

Der Hauptunterschied zwischen wesentlichen und wichtigen Einrichtungen besteht in der Überwachung der Einhaltung der Vorschriften. Bei den wesentlichen Einrichtungen, vor allem in wichtigen Sektoren, wird die Überwachung proaktiv sein. Das bedeutet, dass diese Einrichtungen aktiv überwacht werden, ob die geltenden Rechtsvorschriften eingehalten werden. Bei den wichtigen Unternehmen findet die Aufsicht im Nachhinein statt, wenn es Anzeichen für einen Vorfall gibt. Stellt sich nach einem Vorfall heraus, dass das Unternehmen nicht die erforderlichen Maßnahmen ergriffen haben, müssen sie sich auch mit den möglichen Folgen der Nichteinhaltung dieser Rechtsvorschriften auseinandersetzen.



IN WELCHEM SEKTOR IST IHR UNTERNEHMEN TÄTIG?	
Sektoren nach Anhang I	**Sektoren nach Anhang II**
Energie	Post- und Kurierdienste
Verkehr und Transport	Abfallwirtschaft
Bankwesen	Produktion, Herstellung und Handel mit chemischen Stoffen
Infrastruktur für 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	

* Information and Communication Technology

* **Großunternehmen:**
mehr als 250 Mitarbeiter und ein Jahresumsatz von mindestens 50 Millionen Euro (oder eine Bilanzsumme von mindestens 43 Millionen Euro).

Mittelständische Unternehmen:
mehr als 50 und weniger als 250 Beschäftigte und ein Jahresumsatz von nicht mehr als 50 Millionen Euro (oder eine Bilanzsumme von nicht mehr als 43 Millionen Euro).

3. Was können wir von der **NIS2-Richtlinie in der Praxis erwarten?**

Verpflichtungen und Auswirkungen

Die NIS2-Richtlinie verlangt von weiteren Branchen umfangreichere Anforderungen an die Cybersicherheit sowie von wichtigen und wesentlichen Stellen Maßnahmen zum Management von Sicherheitsrisiken. Unter anderem müssen sie Backups erstellen, Risikoanalysen durchführen und sind verpflichtet, Vorfälle mit erheblichen Auswirkungen auf den Betrieb zu melden. Um den Verwaltungsaufwand gering zu halten, ist die Leitung des Unternehmens für die Einhaltung der Vorgaben in der NIS2-Richtlinie verantwortlich.

Diese neue Richtlinie stellt für viele Unternehmen, ob groß oder klein, einen großen Schritt dar. Sowohl die Regierung als auch die Unternehmen werden mehr Verantwortung tragen müssen. Dies hat auch finanzielle Auswirkungen: Das IKT-Budget von Unternehmen, die noch nicht unter die Richtlinie fallen, wird voraussichtlich um maximal 22 Prozent steigen, bei Unternehmen, die bereits unter der Richtlinie arbeiten, um bis zu 12 Prozent. Auch der Verwaltungsaufwand wird zunehmen. Ob sich diese zusätzlichen IKT-Ausgaben lohnen und den Unternehmen aufgrund des höheren Niveaus der Cybersicherheit Wettbewerbsvorteile verschaffen, bleibt abzuwarten.

Es wird davon ausgegangen, dass die NIS2-Richtlinie nicht nur zu einer strengeren Durchsetzung und strengeren Pflicht, sondern auch zu einer besseren Sicherheit der digitalen Wirtschaft in der Europäischen Union und zum Schutz vor Cyberangriffen führen wird.

Zwei Fallbeispiele

1

Das Energieunternehmen **BrightEnergies** mit 500 Mitarbeitern kam nicht umhin, sich bereits mit der Einführung der ersten NIS-Richtlinie mit entsprechenden Sicherheitsauflagen vertraut zu machen. In der nationalen NIS-Gesetzgebung wurde es im zugehörigen Sektor "Energie" als wichtiger Anbieter eingestuft. Der heutige Geschäftsleiter Lennard war in dieser Zeit noch nicht bei BrightEnergies tätig, aber es ist dokumentiert, welche Maßnahmen und Prozesse zu jener Zeit angepasst oder neu eingeführt wurden. Im Jahr 2022 erfuhr er von der neuen NIS-Gesetzgebung, worin ein Energieunternehmen als "wesentliche Organisation" eingeordnet wird. Mit der Einführung der NIS-Gesetzgebung waren bereits einige Änderungen vorgenommen worden. Aufgrund zahlreicher Hackerangriffe in anderen Ländern (z. B. Luxemburg, Italien und Portugal) auf Energieunternehmen will die Chefetage sicherstellen, dass BrightEnergies davon nicht betroffen ist. Der NIS2-Richtlinie wird daher hohe Priorität eingeräumt.

2

Das Abfallverarbeitungs- und Recyclingunternehmen **Waste2Resource** fiel bisher nicht unter die NIS-Richtlinie oder andere Cybersicherheitsvorschriften. In den letzten Jahren wurde jedoch immer deutlicher, dass auch ein Abfallverarbeitungsunternehmen Opfer eines Cyberangriffs werden kann: Ein Konkurrent wurde im Jahr 2021 durch Ransomware tagelang lahmgelegt, wodurch die Müllabfuhr nicht mehr gewährleistet werden konnte. Das IT-Team von Waste2Resource schätzt es, dass das Unternehmen nun unter die NIS2-Richtlinie fällt, hat aber noch eine Menge zu tun. Das Team, das von der neu eingestellten CISO Kayleigh geleitet wird, ist derzeit mit den Vorbereitungen wie der Erstellung einer Risikoanalyse beschäftigt. Auf jeden Fall wissen sie und ihr Team bereits, dass sie im Rahmen der NIS2-Richtlinie als wichtige Einrichtung angesehen werden und daher mit einer Sorgfaltspflicht und einer reaktiven Meldepflicht rechnen müssen.

4. Was bedeutet NIS2 **für Ihre Organisation?**

Wie eingangs erwähnt, wird in der NIS2-Richtlinie zwischen zwei Kategorien unterschieden: wesentliche und wichtige Einrichtungen. Bisher wurde nur zwischen lebenswichtigen Unternehmen, die unter die NIS-Richtlinie fallen, und nicht lebenswichtigen Unternehmen getrennt. Alle Sektoren und Unternehmen, die unter die NIS2-Richtlinie eingeordnet werden, sind für die Gesellschaft von großer Bedeutung. Es würde sie vor große Probleme stellen, wenn diese Unternehmen ihre Aufgaben nicht mehr erfüllen könnten.

Cyber-Angriffe können nicht nur auf Unternehmen, sondern auch auf die Gesellschaft erhebliche Auswirkungen haben. Hier einige Beispiele für größere Attacken:

NotPetya

Die Verbreitung der Ransomware NotPetya im Jahr 2027 führte zu Störungen, unter anderem die Schließung des Rotterdamer Hafens.

2017

Mandemakers gr. & VDL

Bei den Ransomware-Angriffen auf Mandemakers Groep und VDL wurde der Betrieb dieser Organisation erheblich gestört.

2021

Bakker Logistiek

Infolge des Angriffs auf Bakker Logistiek hatten die Supermärkte mehrere Tage lang keinen Käse in ihren Regalen.

2021

Kaseya

Die Attacke auf den Softwareentwickler Kaseya verschaffte Cyberkriminellen Zugang zu den Systemen tausender Unternehmen.

2021

Die beiden Kategorien sind entwickelt worden, weil nicht alle Sektoren bei einem Sicherheitsvorfall die gleichen Auswirkungen auf das jeweilige System hätten. Im Folgenden veranschaulichen wir den Unterschied zwischen beiden Gruppen - wesentlich und wichtig - und welchen Einfluss diese Differenzierung auf die Änderungen hat, die die NIS2-Richtlinie mit sich bringt.

Sorgfaltspflicht und Berichterstattung

Alle Unternehmen, die unter die NIS2-Richtlinie fallen - wesentlich oder wichtig - müssen ihrer auferlegten Sorgfaltspflicht nachkommen. Es gibt eine Liste von Maßnahmen, die sie mindestens einhalten müssen:

- Strategien für die Risikoanalyse und die Sicherheit von Informationssystemen
- Beachtung des Krisenmanagements und der Betriebskontinuität im Falle eines größeren Cybervorfalls
- Gewährleistung der Sicherheit der Lieferkette
- Sorgfaltspflicht zur Gewährleistung der Sicherheit von Netz- und Informationssystemen
- Einsatz von Kryptographie und Verschlüsselung
- Strategien und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen

Die Europäische Kommission behält sich das Recht vor, die Maßnahmen durch delegierte Beschlüsse und Durchführungsbeschlüsse zu konkretisieren und durch zusätzliche Maßnahmen zu ergänzen. Die Mitgliedstaaten haben dann die Möglichkeit, unter Berücksichtigung der nationalen und sektoralen Gegebenheiten bestimmte Maßnahmen vorzuschreiben. Die Meldepflicht wird auch für alle Organisationen und Unternehmen gelten, die unter die NIS2-Richtlinie fallen. Sie bedeutet, dass die betroffenen Einrichtungen den Vorfall innerhalb von 24 Stunden an die zuständige Behörde melden müssen, nachdem sie davon Kenntnis erlangt haben. Darüber hinaus sind sie verpflichtet, einen Abschlussbericht innerhalb einer Monatsfrist vorzulegen.

5. NIS2 in Kurzform

WICHTIG

Wie im Fall von **Waste2Resource**

Mittlere Organisationen, die in einem der 11 "sehr kritischen Sektoren" oder mittlere und große Organisationen, die in einem der 7 "kritischen Sektoren" tätig sind

WESENTLICH

Wie im Fall von **BrightEnergies**

Große Organisationen, die in den "sehr kritischen Sektoren" tätig sind

DIE SORGFALTSPFLICHT

- Aufrechterhaltung eines grundlegenden Niveaus digitaler Sorgfalt und Durchführung von Schulungen zur Cybersicherheit
- Risikobewertung für die Sicherheit von Informationssystemen
- Beachtung des Krisenmanagements und der Betriebskontinuität im Falle eines größeren Cybervorfalls
- Gewährleistung der Sicherheit der Lieferkette
- Sorgfaltspflicht zur Gewährleistung der Sicherheit von Netzwerken und Informationssystemen, einschließlich der Reaktion auf Schwachstellen und deren Berichterstattung
- Gewährleistung der Sicherheit der Personalressourcen, Zugangsrichtlinien und des Schutzes digitaler Bestände
- Einsatz von Kryptographie und Verschlüsselung
- Einführung oder Anwendung einer mehrstufigen Authentifizierung und/oder einer sicheren internen Kommunikation
- Strategien und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen

Reaktive Überwachung **(nach einem Vorfall)**

Proaktive Überwachung **(auch außerhalb von Vorfällen)**

MELDEPFLICHT (IN 3 PHASEN)

- Frühwarnung innerhalb von 24 Stunden
- Meldung des Vorfalls innerhalb von 72 Stunden
- Abschlussbericht nach einem Monat (oder Fortschrittsbericht bei einem laufenden Vorfall)

Bußgeld für die Nichteinhaltung der Sorgfalts- oder Meldepflicht:

- ein maximales Bußgeld mit einem Höchstbetrag von mindestens **7.000.000 Euro**
- oder **mindestens 1,4%** des weltweiten Jahresumsatzes im vorangegangenen Geschäftsjahr; je nachdem, welcher Betrag höher ist

Bußgeld bei Nichteinhaltung der Sorgfalts- oder Meldepflicht:

- ein maximales Bußgeld mit einem Höchstbetrag von mindestens **10.000.000 Euro**
- oder **mindestens 2%** des weltweiten Jahresumsatzes im vorangegangenen Geschäftsjahr; je nachdem, welcher Betrag höher ist

Darüber hinaus können bestehende Genehmigungen vorübergehend ausgesetzt oder eine natürliche Person, wie z. B. der Geschäftsführer zeitweilig suspendiert werden.

5.1 Überwachung

Die beiden Kategorien unterscheiden sich in der Art und Weise, wie die jeweils auferlegten Anforderungen an die Sicherheit überwacht werden. Bei Unternehmen, die als wesentlich eingestuft sind, wird proaktiv kontrolliert, ob sie die Vorgaben erfüllen.

In der zweiten Kategorie, den wichtigen Unternehmen, erfolgt die Überprüfung der Einhaltung der Vorgaben reaktiv. Das bedeutet, dass erst nach einem Sicherheitsvorfall untersucht wird, ob sie die Rechtsvorschriften und Anforderungen einhalten. Stellt sich im Nachhinein heraus, dass nicht genügend Maßnahmen ergriffen und die Vorgaben nicht erfüllt wurden, können die gleichen Strafen wie bei den wichtigen Einrichtungen verhängt werden.

5.2 Meldung von Cyber-Vorfällen

Die NIS2-Richtlinie sieht für die Meldung von Vorfällen einen "dreistufigen Ansatz" vor. Die "Frühwarnung" innerhalb von 24 Stunden zielt darauf ab, die potenzielle Ausbreitung von Sicherheitsvorfällen zu begrenzen und es den Einrichtungen zu ermöglichen, Unterstützung zu suchen. Die "Vorfallmeldung" innerhalb von 72 Stunden muss eine erste Bewertung des Sicherheitsvorfalls enthalten, in der die Schwere und Auswirkungen sowie Indikatoren für eine Kompromittierung angegeben werden. Der Abschlussbericht nach einem Monat muss sicherstellen, dass Lehren aus früheren Vorfällen gezogen werden können. Dieser Ansatz bezweckt, die Widerstandsfähigkeit einzelner Einrichtungen und ganzer Sektoren gegenüber Cyber-Bedrohungen schrittweise zu verbessern. Abgesehen von der Verpflichtung, die Frühwarnung zu übermitteln, liegt der Schwerpunkt bei der Meldepflicht von Vorfällen auf dem Umgang mit ihnen.

1) Frühwarnung: Unverzüglich und in jedem Fall innerhalb von 24 Stunden nach Kenntnisnahme eines erheblichen Sicherheitsvorfalls muss eine Frühwarnung an die zuständige Aufsichtsbehörde erfolgen. Darin muss angegeben werden, ob der Vorfall auf eine rechtswidrige oder böswillige Handlung zurückzuführen ist oder ob er grenzüberschreitende Auswirkungen haben könnte. Dies sind die unbedingt erforderlichen Informationen. Innerhalb von 24 Stunden nach Einreichung dieser Warnung erhält die meldende Stelle eine Antwort mit einer ersten Rückmeldung von der zuständigen Aufsichtsbehörde oder dem CSIRT (Computer Security Incident Response Team). Wenn die meldende Stelle es wünscht, kann sie eine Anleitung für die Umsetzung möglicher Abwehrmaßnahmen und gegebenenfalls zusätzliche technische Unterstützung erhalten. Kommt es zu einem strafrechtlich relevanten Vorfall, erhält die meldende Stelle auch eine Anleitung, wie sie den Vorfall den Strafverfolgungsbehörden melden kann.

2) Meldung eines Zwischenfalls: Die Meldung eines Sicherheitsvorfalls muss unverzüglich und auf jeden Fall innerhalb von 72 Stunden nach Kenntnisnahme des erheblichen Sicherheitsvorfalls erfolgen. Sie sollte die mit der Frühwarnung übermittelten Informationen aktualisieren und eine (i) erste Bewertung des erheblichen Sicherheitsvorfalls, (ii) einschließlich seines Schweregrads und seiner Auswirkungen, sowie - sofern verfügbar - (iii) die Indikatoren für eine mögliche Kompromittierung von Systemen enthalten.

3) Abschlussbericht: Schließlich wird innerhalb eines Monats nach der Meldung des Sicherheitsvorfalls ein Abschlussbericht vorgelegt, der (i) eine ausführliche Beschreibung des Sicherheitsvorfalls, seines Schweregrads und seiner Auswirkungen, (ii) die Art der Bedrohung bzw. die zugrunde liegende Ursache, die den Sicherheitsvorfall wahrscheinlich ausgelöst hat, (iii) getroffene und laufende Abhilfemaßnahmen und (iv) gegebenenfalls die grenzüberschreitenden Auswirkungen des Sicherheitsvorfalls enthält. In begründeten Fällen und in Absprache mit der zuständigen Aufsichtsbehörde kann von der 24-Stunden-Frist für die Meldung des Vorfalls und der einmonatigen Frist für den Bericht abgewichen werden.

Anwendungsfälle

Bei **BrightEnergies** herrscht eine Krise. Ein Angreifer ist in das Netzwerk eingedrungen, niemand weiß, wie das möglich war und was zu diesem Zeitpunkt hätte unternommen werden müssen. Und dann kann der CISO nicht erreicht werden! Es herrscht ein großes Durcheinander und ein IT-Spezialist übernimmt stellvertretend das Ruder. Er sendet innerhalb von 24 Stunden eine Frühwarnung an die niederländische Aufsichtsbehörde für Digitale Infrastruktur (RDI). Zusammen mit einem externen Dienstleister wird sorgfältig nach den Backups des Unternehmens gesucht. Sie werden gefunden und das Unternehmen weiß, wie es schlimmere Folgen verhindern kann, da es Zugang zu seinen wichtigen Daten hat. Trotzdem ist der Betrieb für Tage unterbrochen, mit allen denkbaren Folgen. Einen Monat nach dem Vorfall werden in einem Abschlussbericht eine ausführliche Beschreibung, Abhilfemaßnahmen und die Grundursache genannt. Die Tatsache, dass im Hinblick auf die Gewährleistung der Sicherheit nicht alles ausreichend geregelt war, hat dem Unternehmen die Augen geöffnet. Diese Krise hat ernste Folgen für BrightEnergies.

Waste2Resource ist mit einem Ransomware-Angriff konfrontiert, genau wie sein Konkurrent im Jahr 2021. Dank der Prozesse, die CISO Kayleigh dokumentiert haben wollte, kann das IT-Team schnell ein aktuelles Backup wiederherstellen. Knapp 24 Stunden später ist die Organisation wieder einsatzbereit. Angesichts der Bemühungen, die Anforderungen der NIS2-Richtlinie zu erfüllen, ist der Schaden nicht allzu groß. Der CISO hat nur eine Sache vergessen: die Frühwarnung. Glücklicherweise hat Kayleighs Teamkollege noch in letzter Minute darauf hingewiesen, dass die Frühwarnung innerhalb von 24 Stunden erfolgen und auch eine Abschlussmeldung vorgelegt werden muss.

6. Erhebliche **Cyber-Bedrohungen**

In der NIS2-Richtlinie wurden strengere Regeln für die Meldung von Sicherheitsvorfällen mit schwerwiegenden Folgen festgelegt. Organisationen sollen auch jede erhebliche Cyber-Bedrohung melden, die zu einem bedeutenden Sicherheitsvorfall führen könnte. Hinsichtlich des Konzepts für Cybersicherheit steht die NIS2-Richtlinie im Einklang mit der Definition der Europäischen Union für Cybersicherheit und der IT-Zertifizierung. Ein Vorfall gilt als bedeutend, wenn er zu einer erheblichen Betriebsunterbrechung oder zu finanziellen Verlusten für die Organisation oder das Unternehmen führt oder er einen massiven materiellen oder immateriellen Schaden für Einzelpersonen oder Organisationen verursachen könnte.

Freiwillige Meldungen

Organisationen, die nicht in den Anwendungsbereich der NIS2-Richtlinie fallen, können freiwillig erhebliche Sicherheitsvorfälle, Cyber-Bedrohungen oder Beinahe-Vorfälle melden. Die Aufsichtsbehörde verfolgt das Meldeverfahren. Bei freiwilligen Meldungen sollten keine zusätzlichen Verpflichtungen auferlegt werden.

Umfang der Pflichten

Die Europäische Kommission kann weitere Leitlinien zu den Informationen, zum Format und Meldeverfahren sowohl für schwerwiegende Sicherheitsvorfälle als auch Cyber-Bedrohungen bereitstellen. Der Geltungsbereich der Verpflichtungen kann daher erweitert werden.

Bußgelder und Strafen

Die Sorgfaltspflicht und die Meldepflicht stellen auch eine Form der Durchsetzung dar, um die geltende Einhaltung der Vorschriften sicherzustellen. Den Behörden stehen dafür verschiedene Aufsichtsmaßnahmen und Ressourcen zur Verfügung.

Mindeststrafen

Die NIS2-Richtlinie enthält eine verbindliche Liste von Strafmaßnahmen, darunter Vor-Ort-Kontrollen, Sicherheitsaudits, Sicherheitsscans, Informationsanfragen und Auskunftsersuchen. Einige Strafen sind für alle Länder gleich, andere nicht, wie beispielsweise für schwere Verstöße. In solchen Fällen müssen die Länder selbst für geltende, verhältnismäßige und durchsetzbare Auflagen sorgen. Auch die Art der Strafmaßnahmen (strafrechtlich oder verwaltungsrechtlich) wird von den Ländern selbst bestimmt. Sie sollten der Schwere und der Art des Verstoßes angemessen sein und Faktoren wie den verursachten Schaden, die Zusammenarbeit mit der zuständigen Behörde und andere Umstände berücksichtigen.

Geldbußen

Anstelle von oder zusätzlich zu den anderen Maßnahmen können je nach den Umständen des Falles Geldbußen von bis zu 10 Millionen Euro oder 2% des weltweiten Jahresumsatzes des Unternehmens geahndet werden, je nachdem, welcher Betrag höher ist. Die nationalen Aufsichtsbehörden müssen ihre eigenen Richtlinien für die Verhängung von Geldbußen entwickeln.

GELDBUßEN

Die NIS2-Richtlinie sieht Geldbußen von bis zu 10 Millionen Euro oder 2% des weltweiten Gesamtumsatzes vor.

SUSPENDIERUNGEN

Personen mit entsprechenden Befugnissen oder Führungskräfte können suspendiert werden.

Anwendungsfälle

BrightEnergies muss nach dem Ransomware-Angriff mit Strafen rechnen. Als wichtiges Unternehmen sind sie verpflichtet, über modernste Sicherheitsmaßnahmen zu verfügen. Der CISO wird suspendiert und es folgt eine saftige Geldstrafe. Der Geschäftsleiter kommt zu dem Schluss, dass die Sicherheit für die IT-Teams ab jetzt oberste Priorität hat und will fortschrittliche Sicherheitslösungen zur proaktiven Verhinderung von Angriffen einführen.

Glücklicherweise kann **Waste2Resource** etwaige Strafen vermeiden. Der Vorfall hat Kayleigh die Augen geöffnet, weswegen sie den CEO um etwas mehr Budget bittet, um das Unternehmen noch besser abzusichern. Auch wenn er sich der Bedeutung bewusst ist, ist er schon recht zufrieden: "Wir erfüllen die Anforderungen doch schon ganz gut, oder?" Nichtsdestotrotz wird das Budget leicht erhöht, um die Sicherheit weiter zu verbessern.

Gemeinsam für mehr Cyber-Resilienz in der EU

Darüber hinaus wird die NIS2-Richtlinie dafür sorgen, dass ein Europäisches Netzwerk der Verbindungsorganisationen für Cyberkrisen (EU-CyCLONe) eingerichtet wird, welches im Falle eines groß angelegten Cyber-Angriffs Unterstützung und Koordination in der EU bietet. Die Experten werden auch darauf bestehen, dass die Mitgliedstaaten zusammenarbeiten und voneinander lernen, um Tipps weiterzugeben und das gegenseitige Vertrauen zu stärken.

7. Wir unterstützen Sie
bei der Umsetzung der NIS2-Richtlinie

Das kann ESET für Ihr Unternehmen tun

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

Über Eversheds Sutherland

Als eine der Top 10 weltweit führenden Anwaltskanzleien bietet Eversheds Sutherland Rechtsberatung und Lösungen für internationale Mandanten, zu dem einige der größten multinationalen Unternehmen der Welt gehören. Die Experten helfen Ihnen bei der Interpretation der Auswirkungen von NIS2 auf Ihr Unternehmen und der Umsetzung pragmatischer Strategien zur Einhaltung der Vorschriften. Sollte es zu einem Cyberangriff kommen, kann die Anwaltskanzlei auf eine langjährige Erfahrung in der Unterstützung globaler Kunden bei ihren Compliance-Projekten und der Reaktion auf Vorfälle zurückblicken.

ESET 100% Made in EU IT-Security

ESET Lösungen für NIS2-Compliance

Übrigens: Die NIS2-Richtlinie sieht für die unter die Richtlinie fallenden privaten und öffentlichen Einrichtungen **umfangreiche Berichtspflichten** vor. Dazu gehört, dass Einrichtungen laut Art. 23, Abs. 4 NIS2-Richtlinie einen Sicherheitsvorfall **innerhalb von 24 Stunden** der zuständigen Behörde melden müssen, wenn er einen erheblichen Einfluss auf die Funktionsfähigkeit der Systeme und Dienste des Unternehmens haben kann. **Innerhalb von 72 Stunden** sollen zudem **Kompromittierungsindikatoren** (IoCs) benannt werden und **nach einem Monat soll ein Abschlussbericht** vorgelegt werden. Bei der Bereitstellung solch umfangreicher Dokumentationen können Endpoint Detection & Response (EDR) Lösungen wie ESET Inspect unterstützen.

Wichtige Hinweise:

In der folgenden Übersicht nutzen wir die Formulierungen aus der NIS2-Richtlinie der Europäischen Union. Die erforderliche Umsetzung in nationales Recht steht sowohl für Deutschland als auch für Österreich noch aus. Es ist jedoch zu erwarten, dass die in Artikel 21 der NIS2-Richtlinie genannten Maßnahmen übernommen werden.

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.

Digital Security
Progress. Protected.

Art. 21, Abs. 2 NIS2-Richtlinie:

„Die in Absatz 1 genannten Maßnahmen müssen auf einem gefahrenübergreifenden Ansatz beruhen, der darauf abzielt, die Netz- und Informationssysteme und die physische Umwelt dieser Systeme vor Sicherheitsvorfällen zu schützen, und zumindest Folgendes umfassen:“

NIS2-Richtlinie im Wortlaut	Unser Ansatz für eine mögliche Umsetzung	ESET Lösung	ESET PROTECT Bundles			
			MDR Ultimate	MDR	Elite	Complete
a) Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme;	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	✓	✓	✓	✓
b) Bewältigung von Sicherheitsvorfällen;	Unser Endpoint 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 Detection & Response 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 Tool wird ESET Inspect mit den nötigen Daten versorgt, um automatisiert auf verdächtige Aktivitäten innerhalb der Unternehmensumgebung zu reagieren.	ESET MDR		✓		
c) 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 Detection & Response Ultimate	✓			

NIS2-Richtlinie im Wortlaut	Unser Ansatz für eine mögliche Umsetzung	ESET Lösung	ESET PROTECT Bundles			
			MDR Ultimate	MDR	Elite	Complete
d) Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren 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	✓	✓	✓	✓
e) Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, 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	✓	✓	✓	✓
f) Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit;	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	✓	✓	✓	✓*
g) grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit;	Für alle Nutzer im Netzwerk können über dynamisch festlegbare Gerätegruppen ganz unkompliziert verschiedene Cyberhygiene-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	✓	✓	✓	✓
	Über ESET PROTECT können Sie für alle Nutzer der Festplattenverschlüsselung Passwortrichtlinien festlegen und durchsetzen. Im Falle des Austritts eines Mitarbeiters lassen sich zudem remote Zugänge zu sensiblen Systemen oder Assets sperren.	ESET Full Disk Encryption	✓	✓	✓	✓
	Unsere kostenlosen Trainings stärken das Bewusstsein für IT-Sicherheit bei allen Mitarbeitenden in Ihrem Unternehmen.	ESET Cybersecurity Awareness Trainings	✓	✓	✓	✓

[1] www.av-comparatives.org/tests/business-security-test-2023-august-november/

* ohne ESET Inspect

NIS2-Richtlinie im Wortlaut	Unser Ansatz für eine mögliche Umsetzung	ESET Lösung	ESET PROTECT Bundles			
			MDR Ultimate	MDR	Elite	Complete
h) Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung;	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	*	*	*	*
i) Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen;	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	*	*	*	*
j) 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 Cloud-Dienste wie Microsoft 365 oder OWA, SAML, FIDO, ADFS 3.0, 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

ÜBER ESET

Als europäischer Hersteller mit mehr als 30 Jahren Erfahrung bietet ESET ein breites Portfolio an Sicherheitslösungen für jede Unternehmensgröße. Wir schützen betriebssystemübergreifend sämtliche Endpoints und Server mit einer vielfach ausgezeichneten mehrschichtigen Technologie und halten Ihr Netzwerk mithilfe von Cloud Sandboxing frei von Zero Day-Bedrohungen. Mittels Multi-Faktor-Authentifizierung und zertifizierter Verschlüsselungsprodukte unterstützen wir Sie bei der Umsetzung von Datenschutzbestimmungen.

Unsere XDR-Basis mit Endpoint Detection and Response-Lösung, Frühwarnsysteme (bspw. Threat Intelligence) und dedizierte Services ergänzen das Angebot im Hinblick auf Forensik sowie den gezielten Schutz vor Cyberkriminalität und APTs. Dabei setzt ESET nicht allein auf modernste Technologien, sondern kombiniert Erkenntnisse aus der cloudbasierten Reputationsdatenbank ESET LiveGrid® mit Machine Learning und menschlicher Expertise, um Ihnen den besten Schutz zu gewährleisten.

3 VON ÜBER 400.000 ZUFRIEDENEN KUNDEN

BVB 09 CHAMPION PARTNER

Seit 2019 ein starkes Team auf dem Platz und digital

Allianz Suisse

Seit 2016 durch ESET geschützt

Mehr als 4.000 Postfächer

ISP Security Partner seit 2008

2 Millionen Kunden

BEWÄHRT

SecurITy made in EU Trust Seal www.kuratorium.de/itsiegel

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

ISO 9001 SGS SYSTEM CERTIFICATION

ISO/IEC 27001 SGS SYSTEM CERTIFICATION

Unsere Lösungen sind nach den Qualitäts- und Informationssicherheitsstandards ISO 9001:2015 und ISO/IEC 27001:2013 zertifiziert

ESET IN ZAHLEN

110.000.000+
Geschützte Nutzer weltweit

400.000+
Geschützte Unternehmen

195+
Länder & Regionen

13
Forschungs- und Entwicklungszentren weltweit

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

welivesecurity by ESET

ESET Digital Security Guide

ESET.DE | ESET.AT | ESET.CH

Digital Security
Progress. Protected.

ESET.DE/NIS2

Stand: 04/2024 | Druck: 04/2024 | Artikelnummer: M_PRINT2024_05