Gutachten zum Entwurf des NIS-2 Umsetzungsgesetzes

und den dazu vom Bundesamt für Sicherheit in der Informationstechnik veröffentlichten Hinweisen

WITH secure

Der Autor Ulrich Emmert

Im Auftrag von WithSecure hat Ulrich Emmert ein neutrales Gutachten zum **NIS-2 Umsetzungsgesetz** erstellt, welches auch die Hinweise des Bundesamts für Sicherheit in der Informationstechnik (BSI) umfasst. Dabei untersucht er auch die potenzielle Umsetzung der NIS-2-Richtlinien mithilfe von Sicherheitslösungen von WithSecure und bewertet diese entsprechend.

Ulrich Emmert ist Rechtsanwalt und Senior Partner der internationalen Partnerschaftsgesellschaft esb Rechtsanwälte Emmert Dr. Bücking Speichert Matuszak-Lesny. Ein Schwerpunkt seiner Tätigkeit sind Beratungen und Schulungen im Bereich des EDV-, Telekommunikations- und Online-Rechts. Dabei kommen ihm seine umfassenden technischen Kenntnisse in den Bereichen Programmierung, Datenbanken und IT-Security zugute. Als qualifizierter Consultant unterstützt Ulrich Emmert Unternehmen auch in den Bereichen Netzwerksicherheit, Softwarelizenz-Verträge sowie Datenschutz. Darüber hinaus ist er Dozent für IT-, Urheber- und Wettbewerbsrecht an der Hochschule für Wirtschaft und Umwelt in Nürtingen, Vorstandsvorsitzender des Verbandes für Organisations- und Informationssysteme e.V. in Bonn, Geschäftsführer des IT-Sicherheits- und Datenschutzberatungsunternehmens esb data GmbH sowie Vorstand der Reviscan AG.

Kontakt:

Ulrich Emmert, Rechtsanwalt
Schockenriedstraße 8 a
70567 Stuttgart

Telefon +49 (0)711 469058-0
E-Mail: ulrich.emmert@kanzlei.de
www.kanzlei.de

Vorwort von WithSecure

Gesetzliche Grundlagen, die wichtigsten Schritte zur NIS-2-Konformität, Maßnahmen und Pflichten

Die Zeit zur Umsetzung der NIS-2-Vorgaben läuft. Dieser Leitfaden stellt Ihnen die gesetzlichen Grundlagen vor und gibt eine Orientierungshilfe zu geeigneten Maßnahmen, mit denen Sie Ihre Cybersicherheit stärken und gleichzeitig NIS-2-konform agieren können. Folgende Themen werden beleuchtet:

- Was ist die NIS-2-Richtlinie und wer ist davon betroffen?
- Welche Pflichten gehen damit einher?
- Welche Maßnahmen sind zur Einhaltung der Vorgaben erforderlich?
- Wie können Unternehmen NIS-2 technisch umsetzen?

Die Einführung von NIS-2 ist ein bedeutender Meilenstein für die IT-Sicherheit. Ziel ist es, dass Unternehmen, Organisationen und Einrichtungen in der EU ihre Cybersicherheit verbessern. Hierzu gehört es:

- Umfassende Resilienz aufzubauen
- Durchgängige Strategien für die Cybersicherheit zu etablieren
- Hohe Sicherheitsstandards zu schaffen
- Cyberangriffe frühzeitig zu erkennen und darauf zu reagieren
- Abwehrmaßnahmen gegen Cyberbedrohungen zu verstärken
- Mechanismen zur Meldung von sicherheitsrelevanten Vorfällen umzusetzen

Schätzungen zeigen, dass etwa 30.000 deutsche Unternehmen von den Vorschriften in NIS-2 betroffen sein werden. Sie müssen strengere Sicherheitsvorkehrungen einführen und deren Durchsetzung sicherstellen. Unternehmen sollten frühzeitig die neuen Regelungen prüfen, um ihre IT-Sicherheit zu stärken, sicherheitsrelevante Vorfälle zu minimieren und sich an die gesetzlichen Anforderungen anzupassen. Dies hilft, Geldstrafen zu vermeiden und die Wettbewerbsfähigkeit zu erhöhen.

WithSecure bietet preisgekrönte Cybersicherheitslösungen für alle Anforderungen

In diesem Leitfaden erfahren Sie, ob Ihr Unternehmen von NIS-2 betroffen ist und erhalten Einblicke in die gesetzlichen Grundlagen. Wir bieten Orientierungshilfen und das notwendige Wissen, um NIS-2-konform zu handeln und Ihr Unternehmen optimal zu schützen. Wir zeigen Ihnen, wie Sie mithilfe von WithSecure sichere Infrastrukturen aufbauen können.

Weitere Informationen erhalten Sie auf unserer Webseite: **www.withsecure.com**

München, September 2024

Inhaltsverzeichnis

Die Grundlagen zu NIS-2

I. Welche Unternehmen, Einrichtungen und Organisationen sind von NIS-2 betroffen?

Die Anwendungsbereiche der 2. Netzwerk- und Informationssicherheitsrichtlinie der Europäischen Union (NIS-2) sind weitreichend. Im Vergleich zur vorherigen Richtlinie (NIS-1) sollen die Regelungen in NIS-2 für Unternehmen in wesentlich mehr Sektoren gelten. Darüber hinaus gibt es weitere Adressaten, wie qualifizierte Vertrauensdienstleister, Top-Level-Domain-Name-Registrierungsstellen, DNS-Dienstleister (DNS: Domain Name System), Telekommunikationsanbieter (TK), kritische Anlagen und Dienststellen der Verwaltung und der Regierung gemäß Anlage 3 „Sektor öffentliche Verwaltung“.

Schätzungen gehen davon aus, dass statt der bisher 2.000 Unternehmen, die von NIS-1 betroffen waren, nun etwa 30.000 Unternehmen von den Regelungen in NIS-2 betroffen sein werden.

Unternehmen sollten diese Regelungen frühzeitig prüfen. Ein Verstoß kann nach den §§ 60 ff. NIS-2 Umsetzungsgesetz-Entwurf mit bis zu zehn Millionen Euro sanktioniert werden. Nach § 38 des Entwurfs kann es auch zu einer persönlichen Haftung der Geschäftsleitung kommen.

In Deutschland wird das BSI-Gesetz (BSI: Bundesamt für Sicherheit in der Informationstechnik) erheblich erweitert, um die Anforderungen der NIS-2-Richtlinie umzusetzen. Ein Referentenentwurf wurde im April 2023 veröffentlicht und im Juli 2023 aktualisiert. Derzeit ist der Regierungsentwurf vom 19.07.2024[1] der aktuelle Stand. Der voraussichtliche weitere Zeitplan bis zum Inkrafttreten des Gesetzes[2] ist folgender:

Bundesrat 1. Durchgang	27. September 2024
Kabinettbeschluss über Gesetzänderung	2. Oktober 2024 mit Nachmeldung
Zuleitung Bundestag	
Bundestag 1. Lesung	10./11. Oktober 2024
Ausschüsse, Anhörung	Beschluss Anhörung 16. Oktober 2024 Anhörung: 4. November 2024 Abschluss IA: 13. November 2024
Bundestag 2./3. Lesung	5./6. Dezember 2024
Bundesrat 2. Durchgang	14. Februar 2025
Inkrafttreten	März 2025

Damit verfehlt Deutschland die von der EU gesetzte Frist zur Umsetzung der Richtlinie um fast 6 Monate, selbst dann, wenn alles im weiteren Gesetzgebungsprozess glatt geht.

[1] https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/kabinettsfassung/CI1/nis2-regierungsentwurf.pdf?__blob=publicationFile&v=1

[2] https://nis2-navigator.de/aktueller-stand-nis2/

Durch das verspätete Inkrafttreten verschieben sich auch die folgenden Fristen des Gesetzes:

Besonders wichtige Einrichtungen

- Registrierung innerhalb von drei Monaten nach Identifizierung §33 (1)
- Teilnahme am Informationsaustausch innerhalb eines Jahres nach Inkrafttreten §30 (7)

Wichtige Einrichtungen

- Registrierung innerhalb von drei Monaten nach Identifizierung §33 (1)

Betreiber kritischer Anlagen

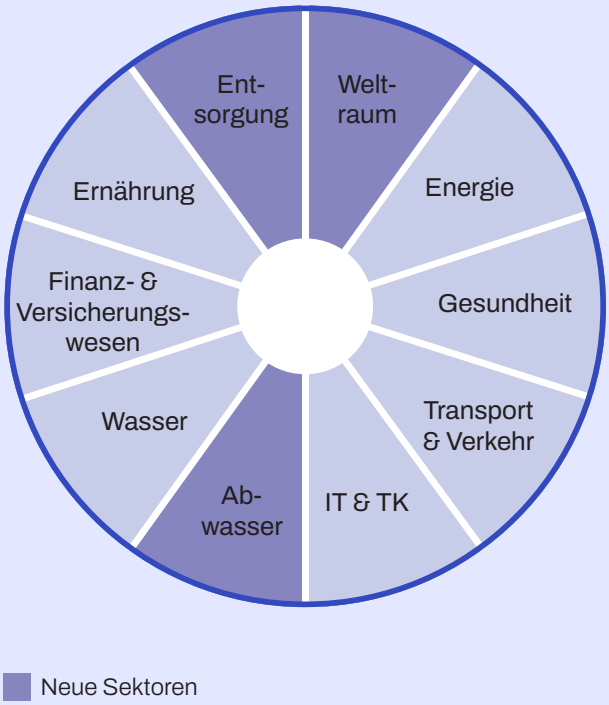
- Registrierung innerhalb von drei Monaten nach Identifizierung §33 (1) und §33 (2)
- Erstmaliger Nachweis über Maßnahmenumsetzung spätestens zu einem vom BSI und BBK bei der Registrierung festgelegten Zeitpunkt: frühestens drei Jahre nach Inkrafttreten des Gesetzes §39 (1)
- Fortlaufende Nachweise über Maßnahmenumsetzung anschließend alle drei Jahre §39 (1)
- Teilnahme am Informationsaustausch innerhalb eines Jahres nach Inkrafttreten §30 (7)

In § 28 ff. des Gesetzentwurfs werden die betroffenen Einrichtungen und Organisationen in drei Stufen beschrieben:

- **Betreiber kritischer Anlagen, bisher als kritische Infrastruktur bezeichnet**
- **Besonders wichtige Unternehmen (inklusive Betreiber kritischer Anlagen)**
- **Wichtige Unternehmen**

Eine „kritische Anlage“ ist nach der Legaldefinition des § 2 Abs. 1 nach dem Entwurf des NIS-2 Umsetzungsgesetzes „eine Anlage, die von hoher Bedeutung für das Funktionieren des Gemeinwesens ist, da durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden; welche Anlagen im Einzelnen kritische Anlagen sind, bestimmt sich nach § 28 Absatz 6“.[3]

Sektoren kritischer Infrastrukturen



[3] https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/referentenentwuerfe/CI1/NIS-2-UmsetzungWirtschaft_DisP.pdf?__blob=publicationFile&v=2

Das geplante KRITIS-Dachgesetz[4] (KRITIS: Kritische Infrastrukturen) soll die Umsetzung der CER-Richtlinie der EU vom 14.12.2022[5] regeln. Es führt zu weiteren Verpflichtungen für Betreiber kritischer Anlagen, die jedoch frühestens 2026 in Kraft treten werden. In neueren Entwürfen des KRITIS-Dachgesetzes und des NIS-2 Umsetzungsgesetzes sind Medien und Kultur sowie die staatliche Verwaltung nicht mehr als KRITIS eingestuft. Für diese Sektoren können Bund und Länder zusätzlich Resilienzmaßnahmen und Monitoring festlegen. In neuen Entwürfen des NIS-2 Umsetzungsgesetzes wurde auch der Sektor „öffentliche Verwaltung“ wieder herabgestuft.

Gemäß § 28 Abs. 1 des NIS-2 Umsetzungsgesetz-Entwurfs gilt eine Einrichtung als **besonders wichtige Einrichtung,** wenn sie entweder mindestens 250 Mitarbeiter beschäftigt oder einen Jahresumsatz von über 50 Millionen Euro und eine Jahresbilanzsumme von über 43 Millionen Euro aufweist. Außerdem zählen qualifizierte Vertrauensdiensteanbieter, Top-Level-Domain-Registries, DNS-Diensteanbieter, Anbieter von Telekommunikationsdiensten oder von öffentlich zugänglichen Telekommunikationsnetzen (mit mindestens 50 Mitarbeitern oder einem Jahresumsatz und einer Jahresbilanzsumme von jeweils über zehn Millionen Euro) sowie Betreiber kritischer Anlagen und Einrichtungen des Teilsektors „Zentralregierung“ des Sektors „öffentliche Verwaltung“ zu den besonders wichtigen Einrichtungen. Ausgenommen sind Finanzunternehmen gemäß Artikel 2 Absatz 2 der Verordnung (EU) 2022/2554 sowie Unternehmen, für die die Anforderungen der Verordnung (EU) 2022/2554 aufgrund von § 1a Absatz 2 des Kreditwesengesetzes oder § 293 Absatz 5 des Versicherungsaufsichtsgesetzes gelten.

Gemäß § 28 Abs. 2 des NIS-2 Umsetzungsgesetz-Entwurfs gelten Einrichtungen **als wichtige Einrichtungen**, wenn sie entweder mindestens 50 Mitarbeiter beschäftigen oder einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über zehn Millionen Euro aufweisen und einer der in Anlagen 1 und 2 bestimmten Einrichtungsarten zuzuordnen sind. Vertrauensdiensteanbieter sind ebenfalls als wichtige Einrichtungen einzustufen. Von dieser Regelung ausgenommen sind jedoch besonders wichtige Einrichtungen sowie Finanzunternehmen gemäß Artikel 2 Absatz 2 der Verordnung (EU) 2022/2554 sowie Unternehmen, für die die Anforderungen der Verordnung (EU) 2022/2554 aufgrund von § 1a Absatz 2 des Kreditwesengesetzes oder § 293 Absatz 5 des Versicherungsaufsichtsgesetzes gelten.

[4] https://ag.kritis.info/wp-content/uploads/2023/07/230717_Referentenentwurf_KRITIS-DachG_vor_Ressortabstimmung.pdf

[5] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2557

II. Verpflichtungen für die IT-Sicherheit

Zu den Verpflichtungen der IT-Sicherheit gehören unter anderem:

1. **Einrichtung eines Informationssicherheitsmanagementsystems (ISMS):** Unternehmen müssen ein ISMS nach ISO/IEC 27001 oder vergleichbaren Standards etablieren und betreiben. Dies umfasst die Festlegung von Richtlinien, Zielen und Prozessen zur Sicherstellung der Informationssicherheit.
2. **Risikomanagement:** Unternehmen müssen regelmäßig Risikoanalysen durchführen, um Schwachstellen und Bedrohungen zu identifizieren und geeignete Maßnahmen zur Risikominimierung zu ergreifen. Dabei müssen sie auch die Auswirkungen von Sicherheitsvorfällen auf die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit berücksichtigen.
3. **Sicherheitsvorfallmanagement:** Unternehmen müssen einen Prozess für das Management von Sicherheitsvorfällen einrichten. Dazu gehört die Überwachung, Erkennung und Reaktion auf Sicherheitsvorfälle sowie die Wiederherstellung des normalen Betriebs nach einem Vorfall.
4. **Schutz vor Malware und Sicherheitslücken:** Unternehmen müssen angemessene technische und organisatorische Maßnahmen ergreifen, um ihre IT-Systeme vor Malware und Sicherheitslücken zu schützen. Dazu gehören regelmäßige Updates, die Implementierung von Firewalls und Virenschutzprogrammen sowie die Schulung der Mitarbeiter zur sicheren Nutzung von IT-Systemen.
5. **Zugangs- und Berechtigungsmanagement:** Unternehmen müssen sicherstellen, dass nur autorisierte Personen Zugriff auf ihre IT-Systeme haben. Dazu gehören die Vergabe und Verwaltung von Zugangsrechten sowie die Überwachung und Protokollierung von Zugriffsaktivitäten.
6. **Awareness- und Schulungsmaßnahmen:** Unternehmen müssen ihre Mitarbeiter regelmäßig über IT-Sicherheitsrichtlinien und -verfahren informieren und schulen. Dadurch soll das Bewusstsein für Sicherheitsrisiken geschärft und das richtige Verhalten der Mitarbeiter gefördert werden.

Diese Verpflichtungen sollen dazu beitragen, die IT-Sicherheit der Unternehmen zu stärken und die Auswirkungen von Sicherheitsvorfällen zu minimieren. Unternehmen, die diesen Verpflichtungen nicht nachkommen, können mit Bußgeldern belegt werden.

In Bezug auf Risikomanagement und Informationssicherheit geht es dabei nach § 30 Abs. 2 um folgende Punkte:

1. Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme
2. Bewältigung von Sicherheitsvorfällen
3. Aufrechterhaltung des Betriebs, wie Back-up-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement
4. Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern (hier gelten gem. § 30 Abs. 8 BSIG-E weitere spezifische Besonderheiten unter Einbeziehung der Entwicklungsprozesse)
5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen
6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit

7. Grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit
8. Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung
9. Sicherheit des Personals, Konzepte für die Zugriffskontrolle und das Management von Anlagen
10. Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie ggf. gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung

Die EU-Kommission kann Durchführungsrechtsakte erlassen, die im Bereich der Sicherheit kritischer Infrastrukturen vorrangig zu beachten sind. Diese Rechtsakte legen fest, welche Maßnahmen Betreiber kritischer Anlagen ergreifen müssen, um die Sicherheit zu gewährleisten. Zusätzlich dazu können besonders wichtige Einrichtungen branchenspezifische Sicherheitsstandards entwickeln, um ihre Verpflichtungen zu erfüllen.

Diese Vorgaben, insbesondere die Punkte 1, 4-6 des 10-Punkte-Katalogs lassen sich meines Erachtens nur mit Hilfe eines **Security and Event Management Systems** umsetzen. Für kritische Infrastrukturen, im Sprachgebrauch des neuen Gesetzes nunmehr „Betreiber kritischer Anlagen“ genannt, ist eine 24x7-Überwachung erforderlich. Aber auch wichtige und besonders wichtige Unternehmen können sich aus meiner Sicht einer täglichen Auswertung der erzeugten Logdaten kaum verschließen, um die Anforderungen des NIS-2 Umsetzungsgesetzes und der NIS-2-Richtlinie zu erfüllen. Für wichtige Unternehmen und besonders wichtige Unternehmen ist ebenfalls eine fachkundige Bewertung der Logdaten notwendig. Hierfür sind auch ohne 24x7-Überwachung mehrere erfahrene Sicherheitsspezialisten erforderlich, die aufgrund ihrer Expertise zu den teuersten Mitarbeitern des Unternehmens zählen dürften. Dabei ist mit der Beauftragung eines Dienstleisters auch ein 24x7-Betrieb ohne exorbitante Kosten möglich. Eine Schadsoftware kann sich heute in nur wenigen Minuten rund um den Erdball auszubreiten – Beispiele liegen zwischen drei und elf Minuten. Ein nächtlich unbeaufsichtigter Betrieb eines SIEM verbietet sich damit. Aus diesem Grund wird es deutlich sinnvoller sein, einen Managed SIEM Service von einem Dienstleister betreiben zu lassen, als SIEM-Software einzukaufen und selbst zu betreiben. Dies gilt unabhängig davon, ob eine ausdrückliche Pflicht zur Angriffserkennung gegeben ist [6] oder nicht, da die Anforderungen von NIS-2 meines Erachtens kaum anders erfüllt werden können.

Betreiber kritischer Anlagen müssen Maßnahmen ergreifen, die über die in § 30 festgelegten Anforderungen hinausgehen, wenn dies angesichts der Auswirkungen eines Ausfalls oder einer Beeinträchtigung noch verhältnismäßig ist.

Im Hinblick auf das Risikomanagement sowie die Erkennung und Reaktion auf Sicherheitsvorfälle müssen besonders wichtige Unternehmen und wichtige Unternehmen **Sicherheitskonzepte** erstellen, um einen sicheren und möglichst störungsfreien Betrieb sowie die Bewältigung von Notfällen zu gewährleisten. Bei der Erstellung dieser Konzepte können die Mindeststandards des Bundesamts für Sicherheit in der Informationstechnik (BSI) nach § 8 des Bundesverfassungsschutzgesetzes (BSIG) oder die Empfehlungen für Telekommunikationsunternehmen im Sicherheitskatalog nach § 167 des Telekommunikationsgesetzes (TKG) herangezogen werden. Das BSI-Grundschutz-Kompendium sowie Sicherheitsmaßnahmen nach den ISO-Normen 27001 ff., insbesondere die ISO-Norm 27002, können ebenfalls verwendet werden.

Des Weiteren müssen Betreiber kritischer Anlagen gemäß § 31 Absatz 2 und § 8a Absatz 1a BSIG (bzw. § 165 Absatz 3 TKG für Telekommunikationsunternehmen) Systeme zur Angriffserkennung bereitstellen. Diese **Systeme zur Angriffserkennung** erfolgen durch den Abgleich von in einem informationstechnischen System verarbeiteten Daten mit Informationen und technischen Mustern, die auf Angriffe hinweisen.

[6] so seit 1.12.2021 für öffentliche TK-Netzbetreiber und seit 1.5.2023 für Betreiber kritischer Anlagen

Bisher in § 8a Abs. 1a BSIG:

„Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen."

Bzgl. der Überprüfung der Einhaltung der Vorschriften des Absatzes 1a heißt es in Absatz 3:

„Betreiber Kritischer Infrastrukturen haben die Erfüllung der Anforderungen nach den Absätzen 1 und 1a spätestens zwei Jahre nach dem in Absatz 1 genannten Zeitpunkt und anschließend alle zwei Jahre dem Bundesamt nachzuweisen. Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen. Die Betreiber übermitteln dem Bundesamt die Ergebnisse der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel. Das Bundesamt kann die Vorlage der Dokumentation, die der Überprüfung zugrunde gelegt wurde, verlangen. Es kann bei Sicherheitsmängeln im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde die Beseitigung der Sicherheitsmängel verlangen."

Die Verschiebung der Pflicht zur Angriffserkennung von § 39 zu § 31 Abs. 2 im neuesten Entwurf des NIS-2 Umsetzungsgesetzes deutet darauf hin, dass die Anforderungen und Zuständigkeiten in Bezug auf die Erkennung von Angriffen neu strukturiert wurden.

Der genaue Inhalt der Regelung in § 31 Abs. 2 ist dabei entscheidend für das Verständnis der Verschiebung. Es wäre daher notwendig, den genauen Wortlaut von § 31 Abs. 2 im aktuellen Entwurf des NIS-2 Umsetzungsgesetzes zu kennen, um die Tragweite dieser Verschiebung besser analysieren zu können. Diese lautet:

„Betreiber kritischer Anlagen sind verpflichtet, Systeme zur Angriffserkennung einzusetzen. Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen. Dabei soll der Stand der Technik eingehalten werden. Der hierfür erforderliche Aufwand soll nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen kritischen Anlage stehen."

Das heißt, dass die Verpflichtungen im Telekommunikationsgesetz und im Energiewirtschaftsgesetz doch nicht in das BSI-Gesetz übertragen werden sollen. Sie sollen stattdessen in den jeweiligen Gesetzen verbleiben.

Aus § 165 Abs. 3 TKG:

„Die eingesetzten Systeme zur Angriffserkennung müssen in der Lage sein, durch kontinuierliche und automatische Erfassung und Auswertung Gefahren oder Bedrohungen zu erkennen. Sie sollen zudem in der Lage sein, erkannte Gefahren oder Bedrohungen abzuwenden und für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorsehen. Weitere Einzelheiten kann die Bundesnetzagentur im Katalog von Sicherheitsanforderungen nach § 167 festlegen."

Die Orientierungshilfe des BSI zum Einsatz von Systemen zur Angriffserkennung bietet eine umfassende Übersicht über bewährte Verfahren und Empfehlungen für den Schutz kritischer Infrastrukturen, Telekommunikations- und Energienetze vor Angriffen.

Die Empfehlungen des BSI zielen darauf ab, die betroffenen Organisationen bei der Auswahl und Implementierung geeigneter Systeme zur Angriffserkennung zu unterstützen. Die Orientierungshilfe beinhaltet Informationen über verschiedene Angriffsarten, die Analyse von Angriffsindikatoren sowie den Einsatz von Schwachstellenscannern und Intrusion-Detection-Systemen.

Darüber hinaus werden Best Practices für die Integration von Angriffserkennungssystemen in die bestehende IT-Infrastruktur, die Erstellung von Sicherheitskonzepten und die Durchführung von Tests und Analysen vorgestellt. Die Orientierungshilfe umfasst auch Aspekte wie die Beurteilung der Effektivität und Effizienz der eingesetzten Systeme sowie die Notwendigkeit einer kontinuierlichen Überwachung und Aktualisierung.

Die Veröffentlichung der Orientierungshilfe bietet den Adressaten nicht nur nützliche Empfehlungen, sondern dient auch als Mittel zur Prüfung der eigenen Sicherheitskonzepte und des Umsetzungsgrads der Angriffserkennungssysteme. So können Unternehmen potenzielle Schwachstellen und Verbesserungsbereiche identifizieren und entsprechende Maßnahmen ergreifen, um die Sicherheit der Informationstechnik zu gewährleisten.

Insgesamt stellt die Orientierungshilfe des BSI einen wichtigen Leitfaden für die Umsetzung effektiver Angriffserkennungssysteme dar und trägt zur Stärkung der IT-Sicherheit in kritischen Infrastrukturen bei.

Folgendes schreibt das BSI in der Einleitung zur Orientierungshilfe:

„Die Betreiber Kritischer Infrastrukturen sowie Betreiber von Energieversorgungsnetzen sind in Deutschland dazu verpflichtet, Angriffserkennung zu leisten, um ihre Informationssysteme zu schützen. Nach einer Neuerung im BSIG und im EnWG müssen Systeme zur Angriffserkennung (SzA) Bestandteil der Nachweise gegenüber dem BSI sein. Das vorliegende Dokument bietet eine Orientierung für Betreiber Kritischer Infrastrukturen sowie prüfenden Stellen zu SzA und den Anforderungen bei deren Umsetzung. Ein Umsetzungsgradmodell zur Bewertung der ergriffenen Maßnahmen und die Nachweiserbringung gegenüber dem BSI werden ebenfalls vorgestellt. Das Dokument eignet sich zudem als Grundlage für die Fortentwicklung der Branchenspezifischen Sicherheitsstandards (B3S) im Zuge der Integration der SzA.“

Zielsetzung und Adressatenkreis der Orientierungshilfe

„Betreiber Kritischer Infrastrukturen haben die Verpflichtung, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen. Das BSIG benennt nach Umsetzung des 2. IT-Sicherheitsgesetzes im neuen § 8a Absatz 1a BSIG nun auch ausdrücklich den Einsatz von Systemen zur Angriffserkennung (SzA). Derartige Systeme stellen eine effektive Maßnahme zur (frühzeitigen) Erkennung von Cyberangriffen dar und unterstützen insbesondere die Schadensreduktion und Schadensvermeidung.

Ziel der vorliegenden Orientierungshilfe SzA ist es, den Betreibern Kritischer Infrastrukturen sowie den prüfenden Stellen einen Anhaltspunkt für die individuelle Umsetzung und Prüfung der Vorkehrungen zu geben.

Zusätzlich soll eine einheitliche Nachweiserbringung gewährleistet werden, indem eine systematische Bewertung der getroffenen Maßnahmen unter Verwendung eines Umsetzungsgradmodells eingeführt wird. Als Bewertungsgrundlage werden die jeweiligen Anforderungen an SzA bzw. deren Umsetzungsgrad verwendet.“

Es wird im Besonderen auf folgende Kapitel aus dem IT-Grundschutz-Kompendium verwiesen:

- OPS.1.1.4 Schutz vor Schadprogrammen
- OPS.1.1.5 Protokollierung
- NET.1.2 Netzmanagement
- NET.3.2 Firewall
- DER.1 Detektion von sicherheitsrelevanten Ereignissen
- DER.2.1: Behandlung von Sicherheitsvorfällen

Der Mindeststandard des Bundesamts für Sicherheit in der Informationstechnik (BSI) zur Protokollierung und Detektion von Cyberangriffen, der gemäß § 8 Abs. 1 BSIG (bald § 44 des BSI-Gesetzes nach dem NIS-2 Umsetzungsgesetz) veröffentlicht wird, gilt auch für die Bundesverwaltung. Dies bedeutet, dass die Bundesverwaltung gemäß diesem Standard Vorgaben zur Protokollierung und Erkennung von Cyberangriffen umsetzen muss. Dieser Mindeststandard stellt somit verbindliche Anforderungen für die Bundesverwaltung dar.

Verbindlich gelten diese Mindeststandards laut § 8 Abs. 1 Satz 1 BSIG für

- *„Stellen des Bundes,*
- *Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie ihrer Vereinigungen ungeachtet ihrer Rechtsform auf Bundesebene, soweit von der jeweils zuständigen obersten Bundesbehörde angeordnet, sowie*
- *öffentliche Unternehmen, die mehrheitlich im Eigentum des Bundes stehen und die IT-Dienstleistungen für die Bundesverwaltung erbringen.“*

Diese Vorgaben sind nicht verbindlich für alle Unternehmen zu befolgen, wie sich im Umkehrschluss ergibt.

Datum	**Mindeststandard**	**Version**
11/2023	Mindeststandard des BSI für die Anwendung des HV-Benchmark kompakt	Version 2.0
06/2023	Mindeststandard des BSI zur Protokollierung und Detektion von Cyberangriffen	Version 2.0
05/2023	Mindeststandard zur Verwendung von Transport Layer Security (TLS)	Version 2.4
12/2022	Mindeststandard zur Nutzung externer Cloud-Dienste	Version 2.1
09/2022	Mindeststandard für Mobile Device Management	Version 2.0
10/2021	Mindeststandard für Videokonferenzdienste	NEU: Version 1.0
07/2021	Mindeststandard für den Einsatz von Schnittstellenkontrollen	Version 1.3

Die technische Umsetzung

Das BSI folgert aus den gesetzlichen Regelungen einen dreistufigen Prozess:

1. Die Protokollierung von betriebs- und sicherheitsrelevanten Ereignissen

Das BSI betrachtet eine zentrale Protokollsammlung mit Agenten auf allen Geräten und eine Normalisierung der Protokolldaten mit Zeitsynchronisation als notwendig für die Erkennung von Angriffen. Es stellt jedoch die Frage, ob dies in allen Fällen ein Security Information and Event Management System erfordert, das die vollständigen Protokolldaten von allen sicherheitsrelevanten Systemen sammelt und Administratoren zentral zur Verfügung stellt. Diese Frage sollte anhand der Informationen aus der „Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung“ und dem Dokument OPS 1.1.5 aus dem Grundschutz-Kompendium beantwortet werden, da auf dieses in der Orientierungshilfe verwiesen wird.

In der Einleitung der Orientierungshilfe heißt es:

> *„Damit ein verlässlicher IT-Betrieb gewährleistet ist, sollten IT-Systeme und Anwendungen entweder **alle oder zumindest ausgewählte betriebs- und sicherheitsrelevante Ereignisse** protokollieren, d. h. sie automatisch speichern und für die Auswertung bereitstellen. Eine Protokollierung wird in vielen Institutionen eingesetzt, um Hard- und Softwareprobleme sowie Ressourcenengpässe rechtzeitig entdecken zu können. Aber auch Sicherheitsprobleme und Angriffe auf die betriebenen Netzdienste können anhand von Protokollierungsdaten nachvollzogen werden. Ebenso können mit solchen Daten durch forensische Untersuchungen Beweise gesichert werden, nachdem ein Angriff auf IT-Systeme oder Anwendungen bekannt wurde.*
>
> *In jedem Informationsverbund werden lokal Protokollierungsdaten von einer Vielzahl von IT-Systemen und Anwendungen generiert. Um jedoch einen Gesamtüberblick über einen Informationsverbund zu erhalten, können die von verschiedenen IT-Systemen und Anwendungen generierten Protokollierungsereignisse an eine dedizierte Protokollierungsinfrastruktur gesendet und dort zentral gespeichert werden. Nur so lassen sich die Protokollierungsdaten an einer zentralen Stelle auswählen, filtern und systematisch auswerten.“*

Dieser Abschnitt erklärt, wie die Protokollierung funktioniert und welche Systeme dafür eingesetzt werden können. Es wird erwähnt, dass zentrale Server für die Logdaten-Sammlung eingesetzt werden können, um Protokolleinträge von sicherheitsrelevanten Systemen zu sammeln und später auszuwerten. Es wird darauf hingewiesen, dass die Daten nachträglich ausgewertet werden müssen, da vor der Übertragung und Speicherung keine Unterscheidung zwischen normalen und auffälligen Logdaten stattfindet. Die Speicherdauer der Logdaten richtet sich nach dem Datenschutzrecht.

Um die Daten einheitlich zu visualisieren, werden oft **Security Information and Event Management Systeme (SIEM)** eingesetzt. Diese Systeme normalisieren und synchronisieren die Daten und stellen sie grafisch dar.

Es müssen die strengen Datenschutzbestimmungen der DSGVO beachtet werden, da bei der Speicherung von Logdaten in der Regel personenbezogene Daten erfasst werden. Es wird erwähnt, dass die Daten nur dann nicht als personenbezogen gelten, wenn die Zuordnungstabellen für dynamisch zugeordnete IP-Adressen nicht verfügbar sind oder gerichtliche Hilfe erforderlich ist[7]. Für Bundesbehörden gelten spezielle Speicherfristen gemäß § 5 des BSI-Gesetzes (zukünftig § 8 des BSI-Gesetzes nach dem NIS-2 Umsetzungsgesetz).

Dieser § 5 des BSI-Gesetzes lautet wie folgt:

„Das Bundesamt darf zur Abwehr von Gefahren für die Kommunikationstechnik des Bundes

- *1. Protokolldaten, die beim Betrieb von Kommunikationstechnik des Bundes anfallen, erheben und automatisiert auswerten, soweit dies zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern bei der Kommunikationstechnik des Bundes oder von Angriffen auf die Informationstechnik des Bundes erforderlich ist,*
- *2. die an den Schnittstellen der Kommunikationstechnik des Bundes anfallenden Daten automatisiert auswerten, soweit dies für die Erkennung und Abwehr von Schadprogrammen erforderlich ist.*

Sofern nicht die nachfolgenden Absätze eine weitere Verwendung gestatten, muss die automatisierte Auswertung dieser Daten unverzüglich erfolgen und müssen diese nach erfolgtem Abgleich sofort und spurenlos gelöscht werden. Die Verwendungsbeschränkungen gelten nicht für Protokolldaten, sofern diese weder personenbezogene noch dem Fernmeldegeheimnis unterliegende Daten beinhalten. Die Bundesbehörden sind verpflichtet, das Bundesamt bei Maßnahmen nach Satz 1 zu unterstützen und hierbei den Zugang des Bundesamtes zu behördeninternen Protokolldaten nach Satz 1 Nummer 1 sowie Schnittstellendaten nach Satz 1 Nummer 2 sicherzustellen. Protokolldaten der Bundesgerichte dürfen nur in deren Einvernehmen erhoben werden.

(2) Protokolldaten nach Absatz 1 Satz 1 Nummer 1 dürfen über den für die automatisierte Auswertung nach Absatz 1 Satz 1 Nummer 1 erforderlichen Zeitraum hinaus, längstens jedoch für 18 Monate, gespeichert werden, soweit tatsächliche Anhaltspunkte dafür bestehen, dass diese im Falle der Bestätigung eines Verdachts nach Absatz 3 Satz 2 zur Abwehr von Gefahren, die von dem gefundenen Schadprogramm ausgehen oder zur Erkennung und Abwehr anderer Schadprogramme erforderlich sein können. Durch organisatorische und technische Maßnahmen ist sicherzustellen, dass eine Auswertung der nach diesem Absatz gespeicherten Daten nur automatisiert erfolgt und dass ein Zugriff auf Daten, die länger als drei Monate gespeichert sind, nur bei Vorliegen tatsächlicher Erkenntnisse über die Betroffenheit des Bundes mit einem Schadprogramm erfolgt. Die Daten sind zu pseudonymisieren, soweit dies automatisiert möglich ist. Eine nicht automatisierte Verarbeitung ist nur nach Maßgabe der nachfolgenden Absätze zulässig. Soweit hierzu die Wiederherstellung pseudonymisierter Protokolldaten erforderlich ist, muss diese durch die Präsidentin oder den Präsidenten des Bundesamtes oder die Vertretung im Amt angeordnet werden. Die Entscheidung ist zu dokumentieren.

[7] EuGH, Urteil vom 19.10.2016, AZ C-482/14

(2a) Protokolldaten dürfen vor ihrer Pseudonymisierung und Speicherung nach Absatz 2 zur Sicherstellung einer fehlerfreien automatisierten Auswertung manuell verarbeitet werden. Liegen Hinweise vor, dass die fehlerfreie automatisierte Auswertung wegen eines erheblichen Fehlers erschwert wird, darf der Personenbezug von Protokolldaten zur Sicherstellung der fehlerfreien automatisierten Auswertung wiederhergestellt werden, sofern dies im Einzelfall erforderlich ist. Absatz 2 Satz 3 bis 6 gilt entsprechend.

(3) Eine über die Absätze 1 und 2 hinausgehende Verwendung personenbezogener Daten ist nur zulässig, wenn bestimmte Tatsachen den Verdacht begründen, dass

- *1. diese ein Schadprogramm enthalten,*
- *2. diese durch ein Schadprogramm übermittelt wurden oder*
- *3. sich aus ihnen Hinweise auf ein Schadprogramm ergeben können,*

und soweit die Datenverarbeitung erforderlich ist, um den Verdacht zu bestätigen oder zu widerlegen. Im Falle der Bestätigung ist die weitere Verarbeitung personenbezogener Daten zulässig, soweit dies

- *1. zur Abwehr des Schadprogramms,*
- *2. zur Abwehr von Gefahren, die von dem aufgefundenen Schadprogramm ausgehen, oder*
- *3. zur Erkennung und Abwehr anderer Schadprogramme erforderlich ist.*

Ein Schadprogramm kann beseitigt oder in seiner Funktionsweise gehindert werden. Die nicht automatisierte Verwendung der Daten nach den Sätzen 1 und 2 darf nur durch einen Bediensteten des Bundesamtes mit der Befähigung zum Richteramt angeordnet werden.“

Der zugehörige § 5a (zukünftig § 9 des BSI-Gesetzes nach dem NIS-2 Umsetzungsgesetz) lautet:

„Das Bundesamt darf zur Abwehr von Gefahren für die Kommunikationstechnik des Bundes und ihrer Komponenten, einschließlich technischer Infrastrukturen, die zum Betrieb der Kommunikationstechnik des Bundes erforderlich sind, Protokollierungsdaten, die durch den Betrieb von Kommunikationstechnik des Bundes anfallen, verarbeiten, soweit dies zum Erkennen, Eingrenzen oder Beseitigen von Störungen, Fehlern oder Sicherheitsvorfällen in der Kommunikationstechnik des Bundes oder von Angriffen auf die Informationstechnik des Bundes erforderlich ist und Geheimschutzinteressen oder überwiegende Sicherheitsinteressen der betroffenen Stellen nicht entgegenstehen. Die Bundesbehörden sind verpflichtet, das Bundesamt bei Maßnahmen nach Satz 1 zu unterstützen und hierbei den Zugang des Bundesamtes zu behördeninternen Protokollierungsdaten nach Satz 1 sicherzustellen. Hierzu dürfen sie dem Bundesamt die entsprechenden Protokollierungsdaten übermitteln. 4§ BSIG § 5 Absatz BSIG § 5 Absatz 1 Satz 5, Absatz BSIG § 5 Absatz 2 bis BSIG § 5 Absatz 4, BSIG § 5 Absatz 8 und BSIG § 5 Absatz 9 gilt entsprechend. 5§ BSIG § 4a Absatz BSIG § 4A Absatz 6 gilt für die Verpflichtung nach Satz 2 entsprechend.“

Zusammenfassung:

Die Möglichkeit, Logdaten für 18 Monate zu speichern, gilt nur für bestimmte Stellen des Bundes. Für andere Stellen gibt es die Grundregel der sofortigen Löschpflicht, es sei denn, es gibt konkrete Anhaltspunkte für einen Missbrauch. Verkehrsdaten dürfen gemäß einem Urteil des Bundesgerichtshofs für sieben Tage aufbewahrt werden – unabhängig von einem konkreten Verdacht. Die Verpflichtung zur Vorratsdatenspeicherung wurde vom Bundesverwaltungsgericht für nicht anwendbar erklärt, da der Europäische Gerichtshof entschieden hatte, dass dies gegen Grundrechte verstößt.

Im Katalog der Sicherheitsanforderungen zu § 167 TKG (vom 29.04.2020, noch zum alten TKG erlassen) heißt es zu Verkehrsdaten im Abschnitt 4.2.2:

„4.2.2 Verkehrsdaten (§ 96 TKG)

Verkehrsdaten sind ebenso wie die Bestandsdaten den personenbezogenen Daten zuzurechnen. Im Gegensatz zu den Bestandsdaten unterliegen die Verkehrsdaten jedoch dem besonderen Schutz von Art. 10 GG bzw. § 88 TKG. Die Vorschrift regelt das datenschutzgerechte Erheben und Verwenden und gibt den pflichtigen Unternehmen gleichzeitig Zulässigkeitsvoraussetzungen vor. U.a. sind dies die folgenden:

- *Das Erheben von Verkehrsdaten kann nur zulässig sein, soweit dies für einen der in Abschnitt 2 von Teil 7 des TKG genannten Zwecke erforderlich ist.*
- *Unter bestimmten weiteren Bedingungen kann die Ermittlung von Kommunikationsprofilen einzelner Teilnehmer und die Analyse von Verkehrsströmen zulässig sein, § 96 Abs. 3 S. 1 TKG.*
- *Die Verkehrsdaten sind i.d.R. vom Diensteanbieter nach Beendigung der Verbindung unverzüglich zu löschen, § 96 Abs. 1 S. 3 TKG. Auf den Leitfaden des/der BfDI und der BNetzA für eine datenschutzgerechte Speicherung von Verkehrsdaten (Stand 19.12.2012) wird verwiesen."*
  (abrufbar unter www.bundesnetzagentur.de/vds)

Aus datenschutzrechtlicher Sicht ist es daher empfehlenswert, Netzwerkdaten gemäß den Bestimmungen von § 30 Nr. 70 TKG nicht vollständig zu protokollieren, sondern die verdächtigen Daten so schnell wie möglich auszusortieren und nur diese zu speichern. Andernfalls müssten die Protokolldaten pseudonymisiert werden.

WithSecure Managed Detection and Response unterstützt die Protokollierung und zeitversetzte Auswertung der Protokolldaten ebenso wie die Just-in-time-Verarbeitung durch eine Kombination von automatischer Erkennungssoftware und Auswertung von Alerts und Offenses innerhalb von 15 Minuten durch Experten, den sogenannten „Threat Huntern" von WithSecure, im Rahmen der Detection & First Response.

Besser als nur die Protokollierung der Logdaten zur späteren Auswertung sind daher Systeme, die eine Live-Angriffserkennung ermöglichen und nur die verdächtigen Daten aufzeichnen.

Dies ist sowohl aus Datenschutzgründen als auch aus Effizienzgründen sinnvoll, da der gesamte Datenverkehr ohne verdächtige Elemente nicht aufgezeichnet werden muss.

Neben SIEM-Systemen mit vollständiger Speicherung aller Logdaten zur zeitversetzten Auswertung sollten daher auch Systeme zur Angriffserkennung eingesetzt werden bzw. solche, die eine Echtzeitanalyse durchführen und nur Logdaten zu verdächtigen Vorfällen langfristig speichern.

Erfahrene Threat Hunter können innerhalb kürzester Zeit – wie oben beschrieben, innerhalb von 15 Minuten – verdächtige Logdaten aussortieren und direkt einer Untersuchung zuführen.

Abweichungen von den Bestimmungen des § 12 TTDSG können aufgrund eines anderen Gesetzes vorgenommen werden. Im BSI-Gesetz gibt es jedoch keine Ermächtigung, die Speicher- und Löschfristen gemäß § 12 TDDSG aufgrund der Verpflichtung zur Angriffserkennung für besonders wichtige Unternehmen oder wichtige Unternehmen zu verlängern, obwohl dies aufgrund der Parallelnormen in § 5 und § 5a des BSI-Gesetzes naheliegend wäre.

Dazu heißt es in der Gesetzesbegründung des NIS-2 Umsetzungsgesetz-Entwurfes lediglich:

> *„Absatz 2 verpflichtet Betreiber Kritischer Anlagen, Systeme zur Angriffserkennung einzusetzen.“*

Es ist wichtig zu beachten, dass dies nur meine Meinung ist und andere Personen möglicherweise eine andere Sichtweise haben können.

Eine Live-Netzwerk- und Prozessanalyse kann dazu beitragen, dass das Datenschutzrecht besser umgesetzt wird, da in diesem Fall Logdaten nicht vollständig gespeichert werden müssen. Bei einer vollständigen Speicherung der Logdaten in einem SIEM-System besteht das Potenzial für eine Verletzung des Datenschutzes, da sensible Informationen gesammelt und gespeichert werden können.

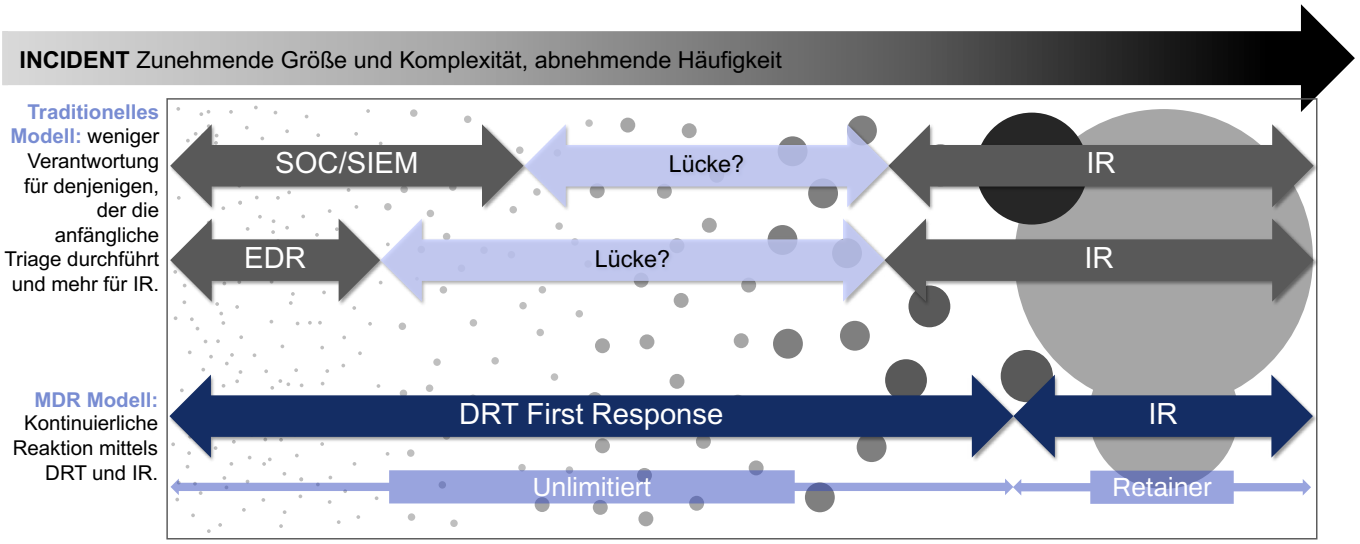


Bild: Die Reaktionslücke bewältigen

Durch die Analyse des Netzwerks und der laufenden Prozesse in Echtzeit können die IT-Verantwortlichen verdächtige Aktivitäten sofort erkennen und darauf reagieren. Dies ermöglicht eine effektive Incident-Response und reduziert die Notwendigkeit einer langfristigen Speicherung von Logdaten.

Die Anforderungen aus dem Gesetz und den Empfehlungen des BSI können meiner Ansicht nach vorrangig durch eine Live-Netzwerk- und Prozessanalyse erfüllt werden. Es ist wichtig sicherzustellen, dass angemessene Sicherheitsmaßnahmen implementiert werden, um den Datenschutz zu gewährleisten. Dies könnte beispielsweise die Pseudonymisierung oder Anonymisierung von Daten und den Einsatz von Schutzmechanismen wie Firewalls oder Intrusion Detection Systems umfassen.

Es ist jedoch zu beachten, dass eine Live-Netzwerk- und Prozessanalyse nicht für alle Organisationen geeignet sein könnte, insbesondere wenn eine umfassende Aufzeichnung von Logdaten zur Erfüllung rechtlicher oder behördlicher Anforderungen erforderlich ist. In diesen Fällen kann eine vollständige Speicherung in einem SIEM-System notwendig sein, um die Compliance sicherzustellen. Auch dies ermöglicht der MDR Service von WithSecure.

Die gesetzliche Vorgabe lautet:

> *„Die Verpflichtung nach Absatz 1 Satz 1, angemessene organisatorische und technische Vorkehrungen zu treffen, umfasst ab dem 1. Mai 2023 auch den Einsatz von Systemen zur Angriffserkennung. Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen.“ (§ 8a Absatz 1a Satz 1, 2 BSIG)*
>
> *„Betreiber Kritischer Infrastrukturen haben die Erfüllung der Anforderungen nach den Absätzen 1 und 1a spätestens zwei Jahre nach dem in Absatz 1 genannten Zeitpunkt und anschließend alle zwei Jahre dem Bundesamt nachzuweisen.“ (§ 8a Absatz 3 Satz 1 BSIG)*

Ebenfalls sind die Schlussfolgerungen in der Orientierungshilfe eingehalten und stellen keinen Widerspruch zur ausschließlichen Protokollierung verdächtiger Logdaten (Alerts und Offenses) dar. Auf Seite 10 der Orientierungshilfe heißt es:

> *„Aufbau zentralisierter Protokollierungsinfrastrukturen:*
>
> *Alle gesammelten sicherheitsrelevanten Protokoll- und Protokollierungsdaten MÜSSEN an für den jeweiligen*

Bild: 24x7 Erkennung und Reaktion

> *Netzbereich zentralen Stellen gespeichert werden. Die Zahl an zentralen Stellen zur Speicherung SOLLTE möglichst geringgehalten werden und sich mindestens an funktionalen Einheiten orientieren, sodass der Zugriff auf die gespeicherten Daten einfach erfolgen kann.*
>
> *Die Protokollierungsinfrastruktur MUSS dazu ausreichend dimensioniert sein. Dafür MÜSSEN genügend technische, finanzielle und personelle Ressourcen verfügbar sein.*
>
> *Bereitstellung von Protokoll- und Protokollierungsdaten für die Auswertung:*
>
> *Die gesammelten Protokoll- und Protokollierungsdaten MÜSSEN gefiltert, normalisiert, aggregiert und korreliert werden. Die so bearbeiteten Protokoll- und Protokollierungsdaten MÜSSEN geeignet verfügbar gemacht werden, damit sie ausgewertet werden können.*
>
> *Eine zeitlich befristete Speicherung der unbearbeiteten Protokolldaten KANN den Detektionsprozess zusätzlich unterstützen.“*

Das Thema der Aufzeichnung und Speicherung von Daten ist in der heutigen digitalen Welt sehr relevant. Es besteht die Notwendigkeit, sicherheitsrelevante Daten aufzuzeichnen, um potenzielle Bedrohungen zu identifizieren und erforderliche Maßnahmen zu ergreifen. Allerdings sollte nicht jedes Detail über eine bestimmte Zeitspanne hinweg aufgezeichnet werden müssen.

Es ist wichtig, zwischen relevanten und irrelevanten Daten zu unterscheiden. Nicht alle Daten sind sicherheitsrelevant oder tragen zur Verbesserung der Sicherheit bei. Zu viele unwichtige Daten können nicht nur die Speicherkapazität belasten, sondern auch einen unverhältnismäßigen Eingriff in die Privatsphäre der Benutzer darstellen.

Die Aufzeichnung von sicherheitsrelevanten Daten sollte sich auf spezifische Informationen konzentrieren, die eine echte Bedrohung darstellen können. Das können beispielsweise Zugriffsversuche auf kritische Infrastrukturen, verdächtige Aktivitäten oder Datenlecks sein. Dank einer gezielten Aufzeichnung dieser Daten können IT-Verantwortliche Sicherheitslücken identifizieren und beheben – ohne eine übermäßige Menge an irrelevanten Informationen zu sammeln.

Es ist wichtig, die Abwägung zwischen Sicherheit und Privatsphäre zu berücksichtigen. Während es von entscheidender Bedeutung ist, Daten aufzuzeichnen, um Sicherheitsprobleme zu erkennen und zu beheben, sollten Unternehmen gleichzeitig angemessene Maßnahmen zum Schutz der Privatsphäre der Benutzer ergreifen. Dies umfasst die Einhaltung der geltenden Datenschutzbestimmungen und die Implementierung von Sicherheitsmechanismen, um sicherzustellen, dass die aufgezeichneten Daten angemessen geschützt sind.

Insgesamt sollte sich die Aufzeichnung von Daten auf sicherheitsrelevante Informationen beschränken, um die Effizienz bei der Identifizierung und Reaktion auf Bedrohungen zu erhöhen, ohne die Privatsphäre der Benutzer unnötig zu beeinträchtigen. Es ist wichtig, einen ausgewogenen Ansatz zu verfolgen, bei dem die Sicherheit gewährleistet ist, ohne dabei die Grundrechte und den Datenschutz zu vernachlässigen.

2. Die Erkennung von sicherheitsrelevanten Vorgängen

Auch die Anforderungen zur Detektion von sicherheitsrelevanten Vorgängen widersprechen diesem Ansatz nicht:

„Kontinuierliche Überwachung und Auswertung von Protokoll- und Protokollierungsdaten:

Alle Protokoll- und Protokollierungsdaten MÜSSEN kontinuierlich überwacht und ausgewertet werden. Dies KANN automatisiert werden, wenn bei relevanten Ereignissen eine unmittelbare Alarmierung der Verantwortlichen gewährleistet ist. Die Prüfung des Ereignisses und ggf. die Reaktion MUSS innerhalb einer der Risikoanalyse entsprechend geringen Zeitspanne erfolgen. Es MÜSSEN Mitarbeitende bzw. Mitarbeitende von Dienstleistern benannt werden, die dafür zuständig sind. Müssen die verantwortlichen Mitarbeitenden aktiv nach sicherheitsrelevanten Ereignissen suchen, z. B. wenn sie IT-Systeme kontrollieren oder testen, MÜSSEN solche Aufgaben in entsprechenden Verfahrensanleitungen dokumentiert sein. Für die Detektion von sicherheitsrelevanten Ereignissen MÜSSEN genügend personelle Ressourcen bereitgestellt werden.

Einsatz zusätzlicher Detektionssysteme: Es MÜSSEN Schadcodedetektionssysteme eingesetzt und zentral verwaltet werden. Anhand des Netzplans MUSS festgelegt werden, welche Netzsegmente durch zusätzliche Detektionssysteme geschützt werden müssen. Insbesondere MÜSSEN die im Netzplan definierten Übergänge zwischen internen und externen Netzen um netzbasierte Intrusion Detection Systeme (NIDS) ergänzt werden.

Infrastruktur zur Auswertung von Protokoll- und Protokollierungsdaten und Prüfung sicherheitsrelevanter Ereignisse: Damit die Protokoll- und Protokollierungsdaten korreliert und abgeglichen werden können, SOLLTEN sie alle zeitlich synchronisiert werden. Die gesammelten Ereignismeldungen MÜSSEN regelmäßig auf Auffälligkeiten kontrolliert werden. Damit sicherheitsrelevante Ereignisse auch nachträglich erkannt werden können, MÜSSEN die Signaturen der Detektionssysteme immer auf aktuellstem Stand gehalten werden.“

Auswertung von Informationen aus externen Quellen:

„Um neue Erkenntnisse über sicherheitsrelevante Ereignisse für den eigenen Informationsverbund zu gewinnen, MÜSSEN externe Quellen herangezogen werden. Da Meldungen über unterschiedliche Kanäle in eine Institution gelangen, MUSS sichergestellt sein, dass diese Meldungen von den Mitarbeitenden auch als relevant erkannt und an die richtige Stelle weitergeleitet werden. Informationen aus zuverlässigen Quellen MÜSSEN grundsätzlich ausgewertet werden. Alle gelieferten Informationen MÜSSEN danach bewertet werden, ob sie relevant für den eigenen Informationsverbund sind. Ist dies der Fall, MÜSSEN die Informationen entsprechend der Sicherheitsvorfallbehandlung eskaliert werden.“

Auswertung der Protokoll- und Protokollierungsdaten durch spezialisiertes Personal:

„Es MÜSSEN Mitarbeitende bzw. Mitarbeitende von Dienstleistern speziell damit beauftragt werden, alle Protokoll- und Protokollierungsdaten auszuwerten. Die Auswertung der Protokoll- und Protokollierungsdaten SOLLTE bei diesen höher priorisiert sein, als ihre übrigen Aufgaben. Daher empfiehlt es sich, dass dies ihre überwiegende

Aufgabe ist. Dieses Personal SOLLTE spezialisierte weiterführende Schulungen und Qualifikationen erhalten. Ein Personenkreis MUSS benannt werden, der für das Thema Auswertung von Protokoll- und Protokollierungsdaten verantwortlich ist."

Zentrale Detektion und Echtzeitüberprüfungen von Ereignismeldungen:

„Es MÜSSEN zentrale Komponenten eingesetzt werden, um sicherheitsrelevante Ereignisse zu erkennen und auszuwerten. Zentrale automatisierte Analysen mit Softwaremitteln MÜSSEN dazu eingesetzt werden, um alle in der Systemumgebung anfallenden Protokoll- und Protokollierungsdaten aufzuzeichnen, in Bezug zueinander zu setzen und sicherheitsrelevante Vorgänge sichtbar zu machen. Alle eingelieferten Protokoll- und Protokollierungsdaten MÜSSEN lückenlos in der Protokollverwaltung einsehbar und auswertbar sein. Die Daten MÜSSEN kontinuierlich ausgewertet werden.

Werden definierte Schwellenwerte überschritten, MUSS automatisch alarmiert werden. Das zuständige Personal MUSS sicherstellen, dass bei einem Alarm nach fachlicher Bewertung und innerhalb einer der Risikoanalyse entsprechend geringen Zeitspanne eine qualifizierte und dem Bedarf entsprechende Reaktion eingeleitet wird. Die Systemverantwortlichen MÜSSEN regelmäßig die Analyseparameter auditieren und anpassen, falls dies erforderlich ist. Zusätzlich MÜSSEN bereits überprüfte Protokoll- und Protokollierungsdaten regelmäßig hinsichtlich sicherheitsrelevanter Ereignisse automatisch untersucht werden.

Als eine zentrale Grundvoraussetzung für die effektive Detektion MÜSSEN zudem Informationen zu aktuellen Angriffsmustern für technische Vulnerabilitäten fortlaufend für die im Anwendungsbereich eingesetzten Systeme eingeholt werden. Dazu MÜSSEN fortlaufend Meldungen der Hersteller (Hard- und Software), von Behörden, den Medien und weiterer relevanter Stellen geprüft werden und in dokumentierte Prozesse des Schwachstellenmanagements einfließen.

Bei der Umsetzung von Detektionsmechanismen SOLLTE initial eine Kalibrierung durchgeführt werden, um festzustellen, welche sicherheitsrelevanten Ereignisse (SRE) im Normalzustand auftreten (Baselining). Dazu SOLLTE bewertet werden, ob dieser Normalzustand in Hinblick auf die Zahl der falsch positiven Meldungen hingenommen werden kann oder ob Änderungen vorzunehmen sind. Die Kalibrierung SOLLTE bei Änderungen innerhalb des Anwendungsbereichs oder der Bedrohungslage erneut durchgeführt werden.

Die SRE MÜSSEN überprüft und dahingehend bewertet werden, ob sie auf einen Sicherheitsvorfall (qualifizierter SRE) hindeuten. Die zur Angriffserkennung eingesetzten Systeme sollten, in eindeutig zuordenbaren Fällen, eine automatisierte Qualifizierung der SRE ermöglichen. Nur qualifizierte SRE SOLLTEN den Prozess der Reaktion auslösen. Die Qualifizierung SOLLTE in automatisiert nicht eindeutig zuordenbaren Fällen manuell durch festgelegte Verantwortliche vorgenommen werden. Basierend auf den gewonnenen Erkenntnissen der Qualifizierung MÜSSEN die Detektionsmechanismen nachjustiert werden.

Sollten branchenspezifisch weitergehende gesetzliche oder regulatorische Anforderungen bestehen, so MÜSSEN diese ebenfalls entsprechend umgesetzt werden."

Die Zeitspanne bis zur Auswertung bezieht sich auf den Prozess der Erfassung und Auswertung von Daten. Falls sich dieser Prozess auf null reduziert und keine Zeit zwischen Erfassung und Auswertung vergeht, können weitere Schäden vermieden werden. Es wird nicht explizit aufgeführt, dass alles aufgezeichnet werden muss, es können auch nur die gefährlichen Vorgänge erfasst und weitergeleitet werden. Diese Daten müssen dann vom zentralen Analysesystem kontinuierlich ausgewertet werden.

Wichtig ist auch die Beurteilung von Bedrohungsszenarien im jeweiligen Kontext. Dies kann von einem ausschließlich maschinellen System selbst unter Verwendung modernster KI-Technologie nicht in der Qualität abgebildet werden wie durch die extrem kurzfristige Beobachtung von Verdachtsfällen durch Spezialisten.

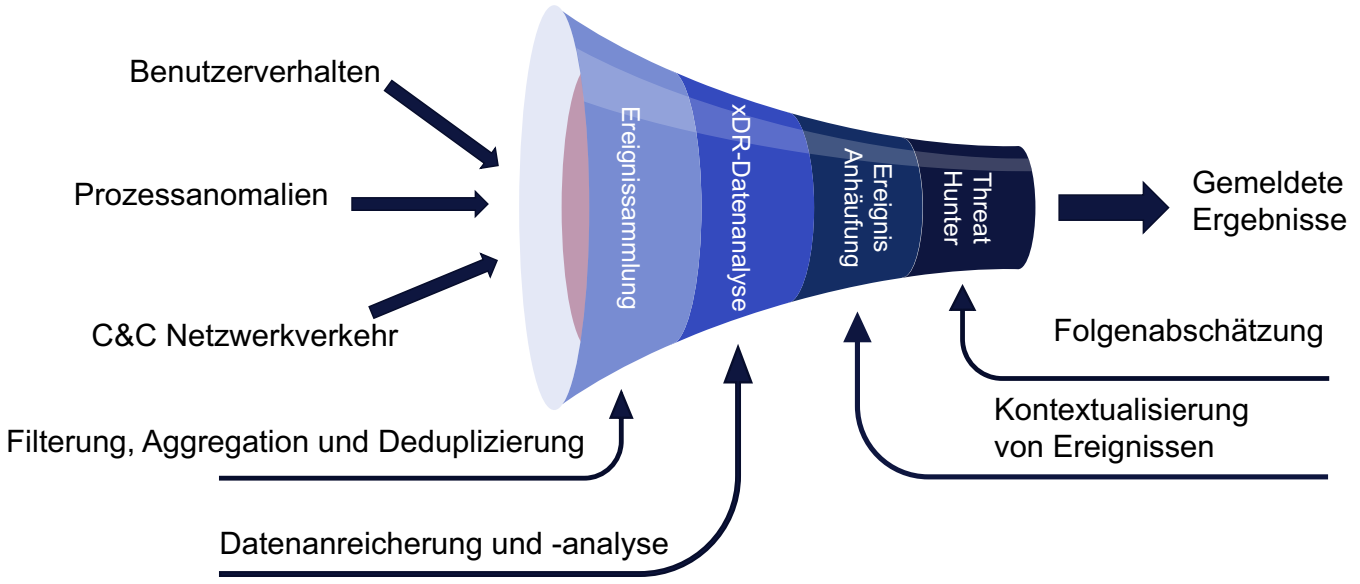


Bild: Der Kontext ist wichtig

3. Die Reaktion auf Bedrohungen und Angriffe

Dies ermöglicht es, Bedrohungen und Angriffe in Echtzeit zu erkennen und Maßnahmen zur Abwehr zu ergreifen. Im Gegensatz zur passiven Netzwerkerkennung, bei der nur der Datenverkehr analysiert wird, erfolgt bei der Live-Netzwerk-Erkennung eine aktive Überwachung des Netzwerks.

Dank des Einsatzes spezieller Hardware und Software können Unternehmen das Netzwerk in Echtzeit überwachen. Dabei werden verschiedene Parameter wie Bandbreitenauslastung, Paketverluste und Latenzzeiten analysiert. So können Abweichungen von normalen Netzwerkaktivitäten erkannt werden, die auf eine mögliche Bedrohung hindeuten könnten.

Die unmittelbare Reaktion ermöglicht es, sofortige Gegenmaßnahmen einzuleiten, um potenzielle Angriffe abzuwehren oder Schäden zu minimieren. So kann das System beispielsweise einen Alarm auslösen, ein infiziertes Gerät isolieren oder einen Netzwerkzugriff für verdächtige IP-Adressen blockieren.

Eine schnelle Reaktion ist besonders wichtig in Zeiten, in denen Cyberangriffe immer raffinierter und komplexer werden. Dank der Echtzeitüberwachung und -erkennung können Unternehmen Sicherheitslücken und Bedrohungen frühzeitig erkennen und bekämpfen, um ihr Netzwerk zu schützen und Schäden zu minimieren.

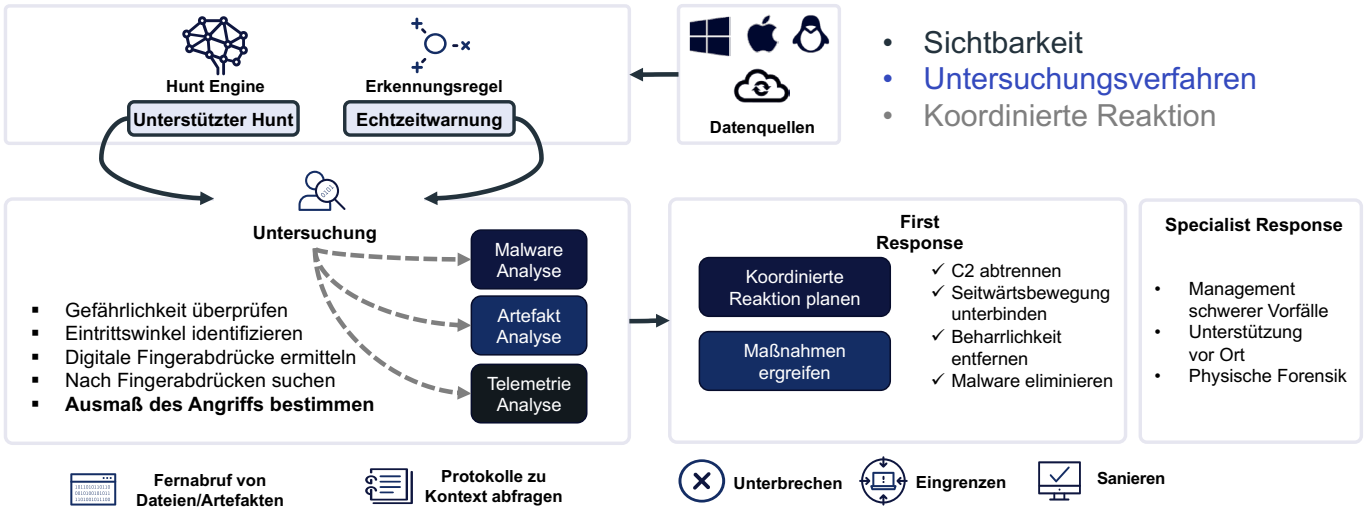


Bild: Wirksame Reaktion

Das Managed Detection and Response System von WithSecure kann die genannten Anforderungen erfüllen, da die Lösung eine Live-Netzwerkanalyse durchführt, um schnelle Reaktionen und Abwehrmaßnahmen gegen Gefährdungen zu ermöglichen. Erfahrene und professionelle Experten, die rund um die Uhr verfügbar sind und die erforderlichen Entscheidungen treffen können, unterstützen das automatisierte Erkennungssystem. Diese Fachleute unterliegen dem EU-Recht, insbesondere dem EU-Datenschutzrecht.

Für Zwecke des innerbetrieblichen Datenschutzes ist die größte Herausforderung, Daten der Mitarbeiter des eigenen Unternehmens bzw. Konzerns zu schützen. Dies ist auch Gegenstand der betrieblichen Mitbestimmung nach den gleichlautenden Vorschriften des Betriebsverfassungsgesetzes bzw. der Personalvertretungsgesetze des Bundes und der Länder. Daher kann eine Pseudonymisierung von Logdaten ausreichend sein, die zwischen der dritten und vierten Säule der untenstehenden grafischen Darstellung eingreift. Denkbar ist jedoch auch, die personenbezogenen Daten wie möglicherweise IP-Adressen schon vor der Untersuchung zu peseudonymisieren, dafür ist der Aufwand jedoch wesentlich höher. Ein Schutzbedürfnis wird regelmäßig angesichts einer noch geringen Verbreitung von IP Version 6 vor allem bei der Auflösung der IP-Adressen eigener Mitarbeiter vorliegen, deren Zugriffe direkt zugeordnet werden können – anhand von internen Adressen, NAT-Umsetzung und DHCP-Lease-Tabellen. Bei der Gestaltung von Sicherheitsrichtlinien und Betriebsvereinbarungen zu SIEM- und Incident Response Systemen (EDR, XDR, UEBA etc.) ist es sinnvoll, auf eine Rechtsberatung durch einen juristisch und technisch versierten Rechtsanwalt, der sich mit dem Thema laufend intensiv beschäftigt, zurückzugreifen.

Für die Aufrechterhaltung des Betriebs und das Krisenmanagement kann das Managed Detection and Response System von WithSecure zum Einsatz kommen. Zusätzliche Maßnahmen im Bereich der IT-Infrastruktur müssen die betroffenen Unternehmen jedoch selbst umsetzen – gemäß den Vorgaben von NIS-2 und dem dazugehörigen Umsetzungsgesetz in Deutschland.

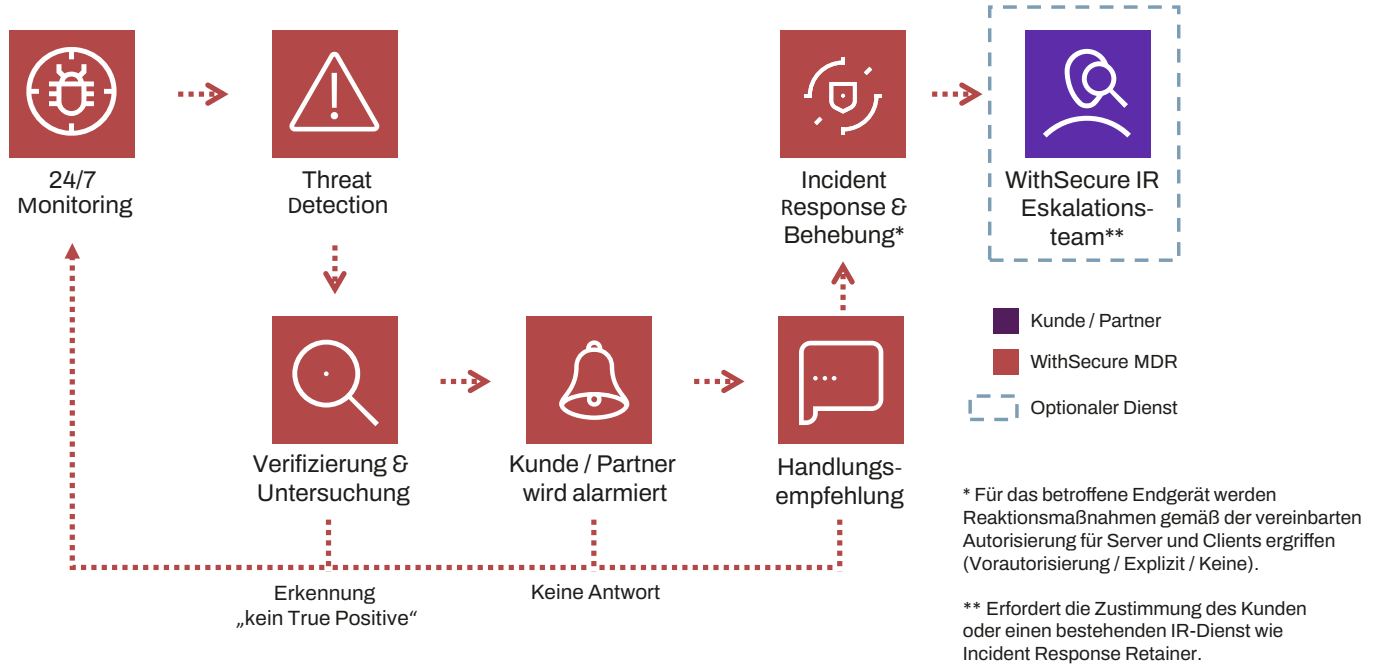


Bild: Wie WithSecure MDR funktioniert

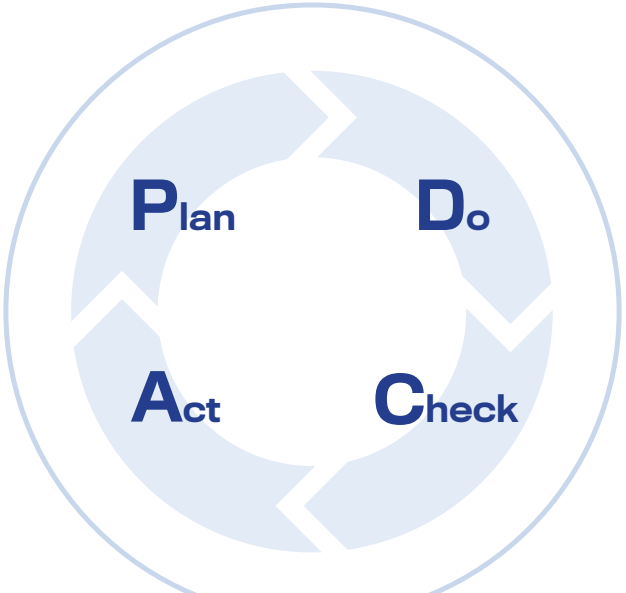
Um die Sicherheit der Lieferkette zu gewährleisten, müssen neben den Betreibern Kritischer Anlagen gemäß § 9b BSIG auch besonders wichtige und wichtige Unternehmen Maßnahmen ergreifen. Das heißt, sie müssen von einem Einsatz von IT- und ITK-Produkten aus fremden Staaten absehen, die möglicherweise für Spionage oder Beeinträchtigungen der IT-Funktionalität genutzt werden können.

In § 20 Abs. 6 des Entwurfs des NIS-2 Umsetzungsgesetzes heißt es nun:

> *„Besonders wichtige Einrichtungen und wichtige Einrichtung dürfen durch Rechtsverordnung nach § 57 Absatz 4 bestimmte IKT-Produkte, IKT-Dienste und IKT-Prozesse nur verwenden, wenn diese über eine Cybersicherheits-zertifizierung gemäß europäischer Schemata nach Artikel 49 der Verordnung (EU) 2019/881 verfügen.“*

Der PDCA-Zyklus (Plan-Do-Check-Act)

Es ist wichtig, dass Unternehmen ihre Sicherheitsmaßnahmen regelmäßig überprüfen und bewerten, um die Effektivität ihres Risikomanagements im Bereich der Cybersicherheit zu beurteilen. Der PDCA-Zyklus beinhaltet die Planung, Umsetzung, Überprüfung und Verbesserung von Sicherheitskonzepten und -verfahren. Dank dieser kontinuierlichen Bewertung können Unternehmen Schwachstellen identifizieren und beheben, um die Sicherheit der informationstechnischen Systeme, Komponenten und Prozesse zu gewährleisten. Sie können auch externe Dienstleister wie Managed Detection and Response-Anbieter hinzuziehen, die sie bei der Erkennung und Reaktion auf Sicherheitsvorfälle unterstützen.



Lizenz CC BY 4.0 | Diagram by Karn G. Bulsuk
www.bulsuk.com

Regelmäßige Schulungen im Bereich der Cybersicherheit dienen dazu, Mitarbeiter für potenzielle Bedrohungen zu sensibilisieren und über aktuelle Sicherheitsmaßnahmen zu informieren. Dies ermöglicht es ihnen, sicherheitsorientiert zu handeln und potenzielle Sicherheitsrisiken zu erkennen und zu melden.

Darüber hinaus ist es wichtig, grundlegende Verfahren der **Cyberhygiene** zu implementieren. Cyberhygiene fasst alle Maßnahmen zusammen, die dazu dienen, dass Unternehmen Cyberangriffe eindämmen beziehungsweise abwehren können und vor Cyberbedrohungen wie Malware geschützt sind. Diese vorbeugenden Routinen und Aktivitäten binden nicht nur Sicherheitsexperten und Administratoren ein, sondern auch die Mitarbeiter. Dazu gehören beispielsweise die regelmäßige Aktualisierung von Software und Betriebssystemen, die Verwendung starker Passwörter, die regelmäßige Überprüfung und Aktualisierung von Zugriffsrechten sowie die Beschränkung des Zugriffs auf sensible Informationen auf autorisierte Mitarbeiter.

Die Kombination von Schulungen im Bereich der Cybersicherheit mit grundlegenden Verfahren der Cyberhygiene kann die Sicherheitskultur im Unternehmen fördern und stärken. Mitarbeiter werden damit zu einem wichtigen Teil der Informationssicherheit und tragen aktiv dazu bei, Sicherheitsvorfälle zu vermeiden.

§ 30 Abs. 2 des NIS-2 Umsetzungsgesetz-Entwurfs

§ 30 Abs. 2 des NIS-2 Umsetzungsgesetz-Entwurfs umfasst zehn Punkte, auf denen die NIS-2-Konformität basiert und die umzusetzen sind. Punkt 8 umfasst die Konzepte für Kryptografie und Verschlüsselung, Punkt 9 die Sicherheit des Personals sowie die Konzepte für die Zugriffskontrolle. Punkt 10 benennt unter anderem die Bedeutung einer Multi-Faktor-Authentifizierung, kontinuierlichen Authentifizierung und gesicherten Kommunikation.

In Bezug auf den Punkt 8 sollten Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung entwickelt werden. Personenbezogene, sicherheitsrelevante und geheimhaltungsbedürftige Daten sollten nur mit starker Verschlüsselung übertragen und gespeichert werden. Mobile Datenträger sollten generell stark verschlüsselte Daten speichern. Dabei sollten die technischen Richtlinien des BSI in Bezug auf Algorithmen und Schlüsselstärke beachtet werden. Unverschlüsselte Prozesse wie der Versand von unverschlüsselten E-Mails sollten durch verschlüsselte Prozesse wie die Nutzung von Secure File Sharing ersetzt werden.

Für Punkt 9 ist es wichtig, rollenbasierte Berechtigungskonzepte mit starker Zugriffskontrolle zu entwickeln. Managementsysteme sollten durch Trennung von offenen Netzen gesichert werden, und in hochsicherheitsrelevanten Bereichen sollte neues Personal gemäß dem Sicherheitsüberprüfungsgesetz oder ähnlichen Maßnahmen geprüft werden. Dabei sollte stets das Verhältnismäßigkeitsprinzip beachtet werden.

Im Hinblick auf Punkt 10 sollten Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung verwendet werden. Passwörter sollten aufgrund der Mehrfachverwendung und des Vergessens eine schlechte Methode der Authentifizierung sein. Für sensiblere Bereiche ist häufig bereits eine 2- oder Multi-Faktor-Authentifizierung vorgeschrieben, daher ist es ratsam, solche Systeme einzuführen. Sprach- und Videokommunikation sollten vor dem Mitlauschen von Dritten oder einsehbaren Transkriptionsfunktionen geschützt sein, insbesondere im Hinblick auf die Möglichkeit einer Auswertung durch Künstliche-Intelligenz-Systeme.

Die organisatorische Gestaltung

III. Pflichten für Meldung, Unterrichtung und Registrierung

1. Meldepflichten

Es ist richtig, dass die Meldepflichten des NIS-2 Umsetzungsgesetzes im Vergleich zu den Meldepflichten der DSGVO bei Datenschutzvorfällen kürzer ausfallen. Das NIS-2 Umsetzungsgesetz bezieht sich speziell auf den Bereich der Cybersicherheit und zielt darauf ab, die Resilienz wesentlicher Dienste und digitaler Dienstleister zu stärken. Angesichts der zunehmenden Bedrohungen und der wachsenden Anzahl von Cyberangriffen ist es wichtig, dass Vorfälle schnell und wirksam gemeldet werden, um angemessene Maßnahmen zum Schutz kritischer Infrastrukturen zu ergreifen.

Die Meldepflichten des NIS-2 Umsetzungsgesetzes sind bewusst kurz gehalten, um eine rasche Information der zuständigen Behörden zu gewährleisten. Dies soll sicherstellen, dass geeignete Maßnahmen zur Abwehr oder Eindämmung des Angriffs ergriffen werden können, bevor größerer Schaden entsteht. Die knappe Formulierung der Meldepflichten ermöglicht es den Betreibern kritischer Infrastrukturen, schnell und unkompliziert eine Meldung abzugeben, ohne sich juristischen Details widmen zu müssen.

Allerdings ist es wichtig zu beachten, dass die Meldepflichten des NIS-2 Umsetzungsgesetzes keine Ausnahme von den Meldepflichten gemäß DSGVO darstellen. Bei einem Sicherheitsvorfall, der auch personenbezogene Daten betrifft, müssen die entsprechenden Meldepflichten der DSGVO weiterhin eingehalten werden. Die Meldepflichten des NIS-2 Umsetzungsgesetzes konzentrieren sich hingegen speziell auf sicherheitsrelevante Vorfälle in digitalen Diensten und wesentlichen Diensten.

Insgesamt lassen sich die kurz gewählten Meldepflichten des NIS-2 Umsetzungsgesetzes als gezielte Maßnahme verstehen, um die Reaktionszeit auf sicherheitsrelevante Vorfälle zu verkürzen und somit die Cybersicherheit insgesamt zu verbessern.

Die Meldepflichten sind in § 32 des Entwurfs des NIS-2 Umsetzungsgesetzes geregelt wie folgt:

> *„Besonders wichtige Einrichtungen und wichtige Einrichtungen übermitteln dem Bundesamt über einen vom Bundesamt im Einvernehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe eingerichteten Meldeweg sowie im Falle von Einrichtungen der Bundesverwaltung zusätzlich der jeweiligen Aufsichtsbehörde:*
>
> *1.* ***unverzüglich, spätestens jedoch innerhalb von 24 Stunden*** *nach Kenntniserlangung von einem erheblichen Sicherheitsvorfall, eine frühe Erstmeldung, in der angegeben wird, ob der Verdacht besteht, dass der erhebliche Sicherheitsvorfall auf rechtswidrige oder böswillige Handlungen zurückzuführen ist oder grenzüberschreitende Auswirkungen haben könnte;*
>
> *2.* ***unverzüglich, spätestens jedoch innerhalb von 72 Stunden*** *nach Kenntniserlangung von einem erheblichen Sicherheitsvorfall, eine Meldung über diesen Sicherheitsvorfall, in der die in Nummer 1 genannten Informationen bestätigt oder aktualisiert werden und eine erste Bewertung des erheblichen Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen, sowie gegebenenfalls die Kompromittierungsindikatoren angegeben werden;*

3. auf Ersuchen des Bundesamtes eine Zwischenmeldung über relevante Statusaktualisierungen;

4. spätestens einen Monat nach Übermittlung der Meldung des Sicherheitsvorfalls gemäß Nummer 2, vorbehaltlich Absatz 2, eine Abschlussmeldung, die Folgendes enthält:

a) eine ausführliche Beschreibung des Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen;

b) Angaben zur Art der Bedrohung beziehungsweise zugrunde liegenden Ursache, die wahrscheinlich den Sicherheitsvorfall ausgelöst hat;

*c) Angaben zu den getroffenen und laufenden Abhilfemaß*nahmen;

d) gegebenenfalls die grenzüberschreitenden Auswirkungen des Sicherheitsvorfalls.

(2) Dauert der Sicherheitsvorfall im Zeitpunkt des Absatz 1 Nummer 4 noch an, legt die betreffende Einrichtung statt einer Abschlussmeldung zu diesem Zeitpunkt eine Fortschrittsmeldung und eine Abschlussmeldung innerhalb eines Monats nach Abschluss der Bearbeitung des Sicherheitsvorfalls vor.

(3) Betreiber kritischer Anlagen sind zusätzlich verpflichtet, Angaben zur Art der betroffenen Anlage, der kritischen Dienstleistung und den Auswirkungen des Sicherheitsvorfalls auf diese Dienstleistung zu übermitteln, wenn ein erheblicher Sicherheitsvorfall Auswirkungen auf die von ihnen betriebene kritische Anlage hat oder haben könnte.

(4) Das Bundesamt kann die Einzelheiten zur Ausgestaltung des Meldeverfahrens und zur Konkretisierung der Meldungsinhalte nach Anhörung der betroffenen Betreiber und der betroffenen Wirtschaftsverbände festlegen, soweit sie möglichen Durchführungsrechtsakten der Europäischen Kommission nicht widersprechen.“

Wenn eine Antwort- oder Reaktionszeit von 24 Stunden vorgegeben wird, ist es wichtig, effektive Prozesse und Meldeketten zu etablieren, um sicherzustellen, dass diese Fristen eingehalten werden können.

Zunächst müssen klare und realistische Ziele für die Reaktionszeit festgelegt werden. Dies kann bedeuten, dass verschiedene Prioritätsstufen definiert werden, je nach Dringlichkeit der Anfrage. Somit weiß das Team, welche Anfragen innerhalb welcher Fristen bearbeitet werden müssen.

Des Weiteren ist es wichtig, die richtigen Kommunikationskanäle für die Meldung von Anfragen zu identifizieren und sicherzustellen, dass diese Kanäle für alle zugänglich und bekannt sind. Dies kann beispielsweise die Einrichtung eines Ticketsystems oder einer speziellen E-Mail-Adresse für Anfragen umfassen.

Um sicherzustellen, dass die Reaktionszeit eingehalten wird, ist es auch notwendig, das Team entsprechend zu organisieren. Dies kann die Zuweisung von bestimmten Mitarbeitern oder Teams zu bestimmten Aufgaben oder Anfragen umfassen, um sicherzustellen, dass jede Anfrage rechtzeitig bearbeitet wird.

Darüber hinaus ist es wichtig, die Workflows und Arbeitsabläufe zu optimieren, um den Prozess der Bearbeitung von Anfragen so effizient wie möglich zu gestalten. Dies beinhaltet möglicherweise die Automatisierung bestimmter Aufgaben oder die Vereinfachung von Genehmigungs- und Eskalationsprozessen.

Schließlich ist es unerlässlich, klare Kommunikationsrichtlinien festzulegen, um sicherzustellen, dass alle relevanten Personen über den Fortschritt informiert sind und Anfragen innerhalb der vorgegebenen Frist beantwortet werden können. Dies kann regelmäßige Statusaktualisierungen oder den Einsatz von Eskalationsverfahren beinhalten, um sicherzustellen, dass dringende Anfragen nicht übersehen werden.

Insgesamt erfordert das Einhalten von Reaktionszeiten von 24 Stunden eine umfassende Planung und ein effektives Projektmanagement, um zu gewährleisten, dass alle Anfragen rechtzeitig bearbeitet werden können. Die Implementierung klarer Prozesse und Meldeketten ist entscheidend, um sicherzustellen, dass die gesteckten Ziele erreicht werden können.

2. Unterrichtungspflichten

In den genannten Sektoren müssen die Empfänger von Diensten, die als besonders wichtig oder wichtig eingestuft sind, über Sicherheitsvorfälle informiert werden. Gemäß Artikel 34 der Datenschutz-Grundverordnung (DSGVO) müssen die Empfänger dieser Dienste informiert werden, wenn ihre Interessen das Interesse der besonders wichtigen oder wichtigen Unternehmen übersteigen. Diese Unterrichtung muss sowohl auf Anordnung des Bundesamts für Sicherheit in der Informationstechnik (BSI) als auch ohne eine solche Anordnung erfolgen.

Es ist daher Aufgabe der Unternehmen in den Sektoren Finanz- und Versicherungswesen, Informationstechnik und Kommunikation, Verwaltung von IKT-Diensten und digitalen Diensten die Empfänger über Sicherheitsvorfälle zu informieren und entsprechende Maßnahmen oder Abhilfemaßnahmen vorzuschlagen, wenn das Interesse der Empfänger höher ist als das Interesse der besonders wichtigen oder wichtigen Unternehmen. Diese Informationspflicht dient der Transparenz und dem Schutz der Nutzer und Kunden dieser Dienste.

3. Registrierungspflichten

Gemäß den §§ 33 und 34 des Umsetzungsgesetzes für die Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen (NIS-2) müssen alle drei Gruppen (KRITIS, besonders wichtige und wichtige Unternehmen) sowie die weiteren besonderen Gruppen sich innerhalb von drei Monaten nach Identifikation ihrer Zugehörigkeit zur jeweiligen Gruppe registrieren lassen. Bei der Registrierung müssen auch die Mitgliedsstaaten innerhalb der EU angegeben werden, in denen das Unternehmen tätig ist.

IV. Haftung und Bußgeld

1. Unternehmen

Hohe Bußgelder dienen der Abschreckung und sollen sicherstellen, dass Unternehmen und Organisationen die Vorschriften des NIS-2 Umsetzungsgesetzes ernst nehmen und angemessene Sicherheitsmaßnahmen treffen, um ihre IT-Systeme und Netzwerke zu schützen.

Es ist wichtig anzumerken, dass die Bußgelder nicht automatisch verhängt werden, sondern von den zuständigen Behörden nach einer gründlichen Untersuchung und Bewertung des jeweiligen Verstoßes festgelegt werden. Die Geldbußen sollen jedoch sicherstellen, dass Verstöße nicht ignoriert werden und dass Unternehmen und Organisationen einen Anreiz haben, in die Verbesserung ihrer Cybersicherheitsmaßnahmen zu investieren.

Es ist ratsam für Unternehmen und Organisationen, die Vorschriften des NIS-2 Umsetzungsgesetzes genau zu studieren, ihre IT-Systeme und Netzwerke auf Schwachstellen zu überprüfen und entsprechende Maßnahmen zu ergreifen, um die Sicherheit ihrer Systeme zu gewährleisten. Die Einhaltung der Vorschriften und die Vermeidung von Verstößen ist eine verantwortungsvolle und kluge Entscheidung, um die Integrität, Vertraulichkeit und Verfügbarkeit ihrer Informationen zu schützen.

2. Geschäftsführung

Die Regelungen gelten für Geschäftsleiter von Unternehmen, die als „besonders wichtige Unternehmen“ oder „wichtige Unternehmen“ eingestuft sind. Die genaue Definition dieser Unternehmen und die Kriterien für diese Einstufung sind im NIS-2 Umsetzungsgesetz festgelegt.

Es ist wichtig zu beachten, dass Geschäftsleiter eine persönliche Haftung für Fehler im Risikomanagement tragen. Dies bedeutet, dass sie persönlich für entstandene Schäden haften und gegebenenfalls mit ihrem Privatvermögen zur Verantwortung gezogen werden können. Diese Haftung kann nicht ausgeschlossen werden, außer im Rahmen eines Insolvenzverfahrens. Darüber hinaus müssen Geschäftsleiter regelmäßig Schulungen zu Risikomanagementthemen besuchen, um ihre Kompetenzen in diesem Bereich auf dem neuesten Stand zu halten.

Es ist anzumerken, dass diese Verpflichtungen unabhängig von der Rechtsform des Unternehmens gelten. Vorstandsmitglieder von Aktiengesellschaften unterliegen bereits nach § 93 AktG ähnlichen Vorschriften.

Insgesamt zielen diese Bestimmungen darauf ab, das Risikomanagement in Unternehmen zu stärken und sicherzustellen, dass Geschäftsleiter angemessen über die Risiken informiert sind und ihre Aufsichtspflichten erfüllen. Die persönliche Haftung soll Anreize für Geschäftsleiter schaffen, ihre Verantwortung ernst zu nehmen und wirksame Risikomanagementmaßnahmen zu implementieren.

V. Datenschutz

WithSecure stellt sicher, dass personenbezogene Daten gemäß den Bestimmungen der Datenschutzgrundverordnung (DSGVO) geschützt werden. Die Daten werden auf Kundenwunsch ausschließlich in der Europäischen Union gespeichert. Auch ohne die Europe-Only-Option trägt WithSecure trotzdem Sorge dafür, dass sowohl WithSecure selbst als auch deren Auftragsverarbeiter Daten ausschließlich nach den Bestimmungen der Art. 45 ff. DSGVO speichern und verarbeiten.

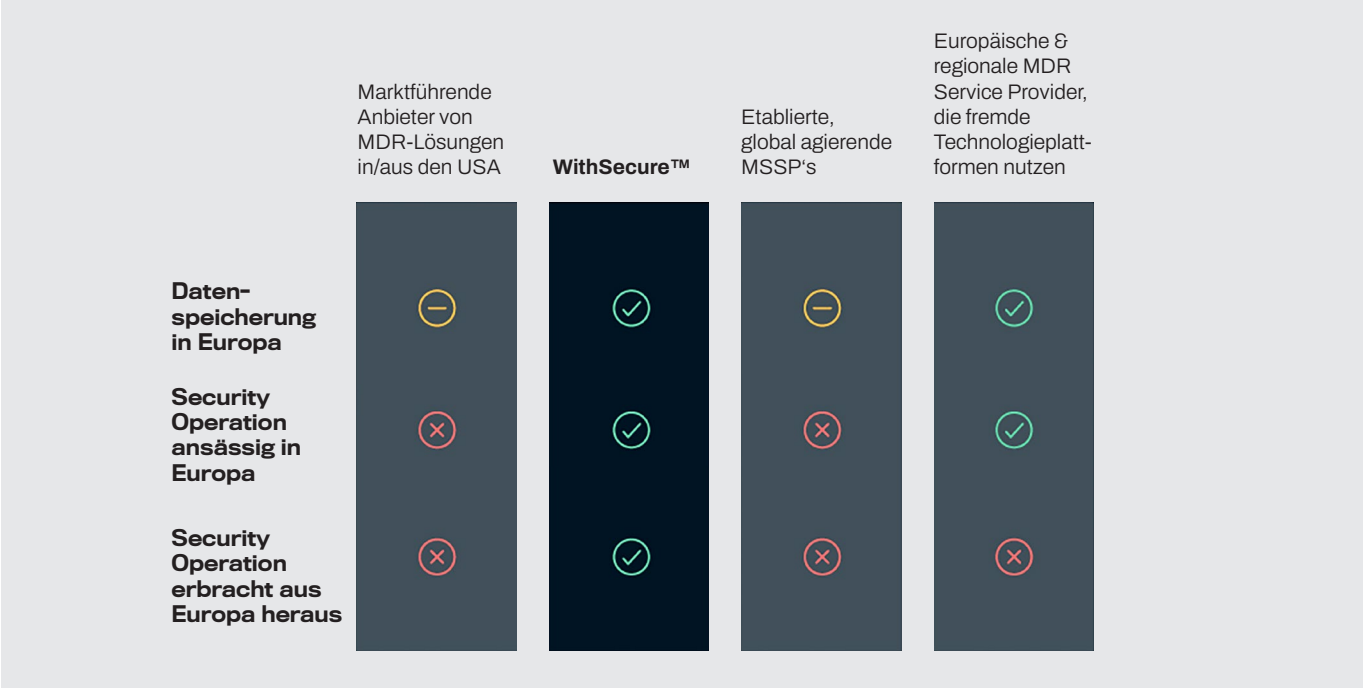


Bild: Europe-only Managed Detection & Response

Fazit

Das NIS-2 Umsetzungsgesetz und das KRITIS-Dachgesetz erhöhen die Anforderungen an die IT-Sicherheit erheblich.

Neue Bußgelder bis zu zehn Millionen Euro sollten für die betroffenen Unternehmen Anlass genug sein, frühzeitig damit zu beginnen, entsprechende Sicherheitskonzepte und Software zu implementieren. Die Geschäftsführung ist nach § 38 des Gesetzentwurfs mit ihrem Privatvermögen haftbar und hat umfassende Überwachungs- und Kontrollpflichten. Nach dem neuesten Entwurf ist sie sogar verpflichtet, persönlich an umfangreichen Schulungen zur Informationssicherheit teilzunehmen.

WithSecure Managed Detection and Response bietet sich beispielsweise dafür an, die neuen und bestehenden gesetzlichen Vorgaben und Richtlinien umzusetzen. KRITIS-Betreiber müssen zudem Systeme zur Angriffserkennung bereitstellen, wofür sich besonders ein System zur Live-Netzwerküberwachung wie WithSecures Managed Detection and Response eignet.

Die 10-Punkte-Liste aus den §§ 30,31 NIS-2 Umsetzungsgesetz bedeutet auch, dass besonders wichtige und wichtige Unternehmen ebenfalls kaum ohne ein solches System auskommen können. Die Ziele des § 30 und § 31 NIS-2 Umsetzungsgesetzes können vielmehr aus meiner Sicht ohne ein solches System nicht oder nur schwer erreicht werden.

Aus Datenschutzsicht ist es empfehlenswert, einen Hersteller aus der EU zu wählen, um Schwierigkeiten im Bereich der Selbstzertifizierung von Herstellern nach dem US-EU Data Privacy Framework oder bei der Erstellung eines Transfer Impact Assessment im Rahmen der Verwendung der EU-Standardvertragsklauseln vom 4. Juni 2021 ausschließen zu können.

Über WithSecure™

WithSecure™, vormals F-Secure Business, ist der bevorzugte Cybersecurity-Partner für IT-Dienstleister, MSSPs und Unternehmen in Europa. Als Experte für outcome-basierte Cybersicherheitslösungen richtet sich das Unternehmen insbesondere an den Mittelstand und legt Wert auf die europäische Art des Datenschutzes, Datenhoheit und regulatorische Compliance.

Mit mehr als 35 Jahren Branchenerfahrung hat WithSecure™ sein Portfolio so gestaltet, dass Kunden und Partner den Paradigmenwechsel von reaktiver zu proaktiver Cybersicherheit bewältigen können. Als partnerorientiertes Unternehmen bietet WithSecure™ flexible Geschäftsmodelle, um gemeinsam die Herausforderungen einer dynamischen Cybersicherheitslandschaft zu meistern.

CYBERSECURITY™
MADE IN EUROPE

Wir folgen dem europäischen Ansatz des Datenschutzes, geprägt von unserem Respekt für Privatsphäre, Datensouveränität und gesetzliche Vorschriften. Seit 1988 in Europa verwurzelt, prägen diese Werte unser tägliches Handeln. So bieten wir Cybersicherheitslösungen speziell für den Mittelstand, die Angriffe effektiv abwehren und Ihre EU-Konformität ab dem ersten Tag gewährleisten.

Die mehrfach ausgezeichnete WithSecure™ Elements Cloud integriert nahtlos KI-gestützte Cybersicherheitstechnologien, menschliche Expertise von Threat Huntern und Analysten sowie Co-Security Services und ermöglicht Unternehmen, die WithSecure™ Produkte für Endpoint- und Cloud-Schutz, Bedrohungserkennung und -reaktion sowie Exposure Management modular und bedarfsgerecht einzusetzen.

WithSecure™ Corporation wurde 1988 gegründet und ist an der NASDAQ OMX Helsinki Ltd. notiert.

www.withsecure.com

NIS2 DORA GDPR ISAE 3000 TYPE II ISO 27001

Cyber-Sicherheitsnetzwerk

Kontaktdaten:

WithSecure GmbH
Niederlassung D/A/CH
Kistlerhofstraße 172c
D-81379 München

E-Mail: vertrieb-de@withsecure.com
Telefon: +49 (0) 89 787 467 0

www.withsecure.com