# Network Information Security (NIS 2)

## Nicht nur KRITIS-Unternehmen im Fokus

Kai-Oliver Detken

Ab Mai 2023 mussten betroffene Unternehmen das 2015 eingeführte Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme von Betreibern kritischer Infrastruktur umgesetzt haben und sogenannte „Systeme zur Angriffserkennung" vorhalten. Ab Oktober 2024 werden diese Vorgaben durch die europäischen Regularien Network and Information Security (NIS 2) und Critical Entitites Resilience Directive (CER) noch einmal verschärft, so dass auch mittlere Unternehmen sich vor Angriffen schützen und diese dokumentieren müssen. Dabei bestehen allerdings Unklarheiten, was die Auswahl und den Betrieb solcher Systeme angehen.

*Durch die europäischen Regelungen Network and Information Security (NIS) und Critical Entities Resilience Directive (CER) kommen einige Änderungen auf betroffene Unternehmen zu (Foto: Gerd Altmann, pixabay)*

Das Sicherheitsgesetz 2.0 ist das zweite Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme und wurde bereits am 23. April 2021 vom Bundesrat verabschiedet. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bekommt dadurch neue Kompetenzen. Unternehmen kritischer Infrastrukturen sind dadurch verpflichtet, Angriffe auf ihr Firmennetz unverzüglich dem BSI zu melden, damit Gegenmaßnahmen empfohlen werden können. Auch müssen erweiterte IT-Sicherheitsmaßnahmen umgesetzt werden. KRITIS-Unternehmen arbeiten daher seit Jahren an einer Umsetzung, um die neuen gesetzlichen Auflagen zu erfüllen. Dies ist keinesfalls trivial, da beispielsweise passende Anomalie-Erkennungssysteme ausgewählt, getestet und implementiert werden müssen, ohne den täglichen Betrieb zu gefährden.

Die Auflistung neuer Sicherheitsverordnungen seit 2015 verdeutlich, dass grundsätzlich Unternehmen immer mehr Auflagen erfüllen müssen, um sich gegen Cyberattacken schützen zu können:

- Sicherheitsgesetz 1.0 (2015): Änderungsgesetz zum BSIG, EnWG, TKG, AtG und TMG. Verpflichtet Betreiber Kritischer Infrastrukturen (KRITIS), ihre IT-Infrastruktur angemessen abzusichern und diese Sicherheit kontinuierlich überprüfen zu lassen.
- BSI-KRITIS-Verordnung (2016): Definition von Sektoren und Schwellenwerten (Bedeutung des Versorgungsgrads).

Prof. Dr.-Ing. Kai-Oliver Detken ist Geschäftsführer der DECOIT GmbH & Co. KG und Dozent an der Hochschule Bremen

- Umsetzungsgesetz NIS 1 (2017): Neue Regelungen für Anbieter digitaler Dienste.
- IT-Sicherheitsgesetz 2.0 (2021): Einsatz von Systemen zur Angriffserkennung (§ 8a Abs. 1a). Neuer Sektor der Siedlungsabfallentsorgung, Selbsterklärung zur IT-Sicherheit für Unternehmen im besonderen öffentlichen Interesse (§ 8f).
- NIS 2 und Resilience of Critical Entities (2024): Definition neuer Sektoren (z. B. öffentliche Verwaltung, Weltraum, Forschungseinrichtungen), Einführung von „Size-Cap-Regeln“, Unternehmen mit über 50 Mitarbeitern oder Jahresumsätze von über 10 Mio. Euro müssen die Sicherheitsregeln ebenfalls umsetzen.
- Digital Operational Resilience Act (2025): Betriebsstabilität digitaler Systeme des Finanzsektors.

Dies ist aufgrund der immer größeren Bedrohungslage auch notwendig, die auch der jährliche BSI-Lagebericht widerspiegelt (siehe Abbildung 1). Demnach waren 66% aller Spam-Mails im Jahr 2023 Cyberangriffe, die 34% Erpressungsmails und 32% Betrugsmails enthielten. Alle betrügerischen E-Mails waren Phishing-Mails zur Erbeutung von Authentifizierungsdaten. Rund 21.000 infizierte Systeme wurden täglich im Jahr 2023 erkannt. Das BSI spricht inzwischen von einer besorgniserregenden Lage.

Dementsprechend werden die gesetzlichen Regularien immer weiter verschärft, was unter anderem durch die europäische NIS 2-Regelung zum Ausdruck gebracht wird, die bis zum 17. Oktober 2024 in die deutsche Gesetzgebung eingebunden werden muss. Die Anzahl der als tatsächlich kritisch eingestuften Unternehmen wird sich dann von ca. 800 auf 30.000 erhöhen. Ob das BSI dieses zusätzliche Arbeitsaufkommen ableisten kann, ist allerdings fraglich.

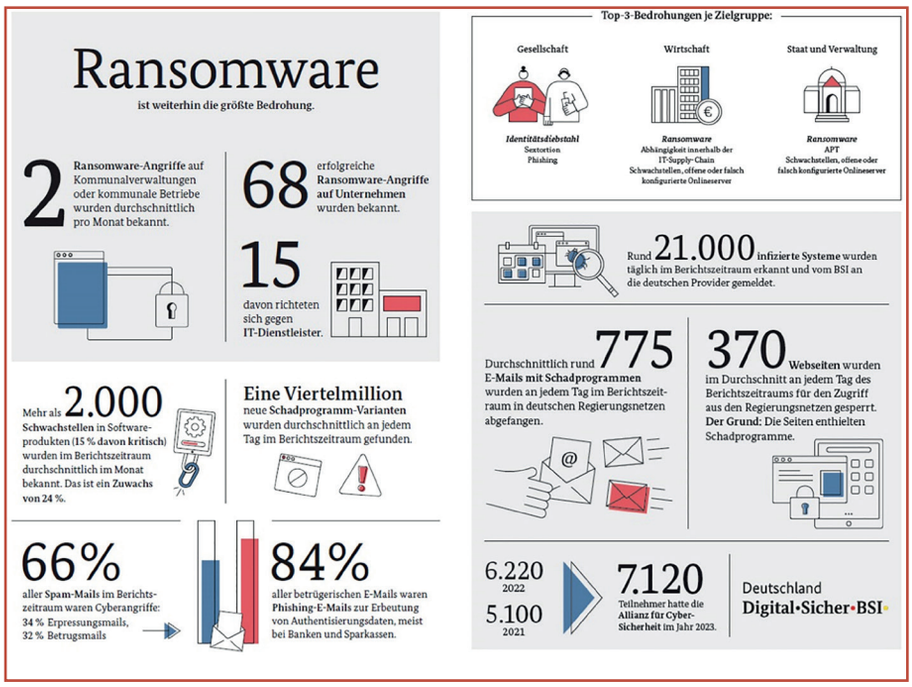


*Bild 1: Laut dem aktuellen BSI-Lagebericht waren 66% aller Spam-Mails im Jahr 2023 Cyberangriffe. Rund 21.000 infizierte Systeme wurden täglich im Jahr 2023 erkannt. Das BSI spricht von einer besorgniserregenden Lage (Grafik: BSI)*

## Neuerungen durch NIS 2

Durch die europäischen Regelungen Network and Information Security (NIS) und Critical Entities Resilience Directive (CER) kommen einige Änderungen auf betroffene Unternehmen zu. Zum einen werden mehr als doppelt so viele Sektoren (18 Stück, wie zum Beispiel Anbieter digitaler Dienste, Post, Forschung, Banken) als kritisch eingestuft. Zum anderen werden gesetzliche Verstöße gegen die NIS 2-Vorgaben nach einem erheblich verschärften Bußgeldkatalog geahndet.

Die wichtigste Neuerung stellt darüber hinaus aber die Geschäftsleiterverantwortlichkeit dar, durch die die Geschäftsführung bei Pflichtverletzungen persönlich haftet. In diesem Fall wird das private Vermögen herangezogen, unabhängig davon, ob die Firma eine Kapital- oder Personengesellschaft mit beschränkter Haftung ist. Ob dies durchsetzbar ist, kann allerdings auch erst die spätere Praxis beantworten, da die Geschäftsführer normalerweise durch Kapitalgesellschaften von direkter Haftung ausgeschlossen werden.

Auch die Meldepflicht bei Sicherheitsvorfällen wurde neu geregelt. Sie soll zukünftig zweistufig erfolgen:

- Innerhalb von 24 Stunden muss eine vorläufige Meldung erfolgen, wenn eine kritische Dienstleistung ausfällt. Das gilt auch, wenn noch keine Kenntnisse darüber vorliegen, was genau passiert ist.
- Spätestens nach 72 Stunden erwartet die BSI-Aufsichtsbehörde eine qualifizierte Meldung über den Vorfall und wie dieser bekämpft werden soll.

Dabei wurde auch die bisherige KRITIS-Verordnung angepasst. Vorher waren Sektor-Zugehörigkeit, Anlagenkategorien und Schwellwerte ausschlaggebend. So legte beispielsweise der Schwellwert von 500.000 Menschen, die von einem Anlagenausfall betroffen wären, fest, ob ein Unternehmen in die KRITIS-Verordnung fiel oder nicht. In NIS 2 wurde die Einstufung hingegen auf Basis der Unternehmensgröße und Umsatzzahlen vorgenommen. Es gilt daher ein einfaches Mengengerüst: Unternehmen aus einem von 18 Sektoren mit mehr als 50

Mitarbeitern oder 10 Millionen Euro Jahresumsatz fallen nun unter die neuen gesetzlichen Regelungen.

NIS 2 verlangt die Einhaltung von zehn Risikomanagementmaßnahmen im Bereich der Cyber-Security:

- Konzepte zur Risikoanalyse und Sicherheit für Informationssysteme
- Bewältigung von Sicherheitsvorfällen
- Aufrechterhaltung des Betriebs (durch z. B. Notfall- und Krisenmanagement)
- Absicherung der Lieferkette
- Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, inklusive Offenlegung der Schwachstellen
- Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementverfahren
- Grundlegende Verfahren im Bereich der Cyberhygiene und Schulung im Bereich der Cybersicherheit
- Konzepte und Verfahren für den Einsatz von Verschlüsselungsverfahren
- Sicherheit des Personals, Konzepte der Zugriffskontrolle und Anlagenmanagement
- Verwendung von Lösungen zur Multi-Faktor-Authentifizierung und gesicherter Sprach-, Video- und Textkommunikation

Des Weiteren wird zwischen wichtigen und besonders wichtigen Einrichtungen unterschieden. Letztere sind Unternehmen, die mehr als 250 Mitarbeiter oder 50 Millionen Euro Jahresumsatz haben. Diese besonders wichtigen Einrichtungen müssen sich wie KRITIS-Betreiber verhalten, weshalb sie zum aktiven Nachweis zur Einhaltung der Regeln verpflichtet werden. Die kleineren Unternehmen unterliegen hingegen keiner regelmäßigen Nachweispflicht. Bei einem Sicherheitsvorfall oder Verdacht können die Aufsichtsbehörden allerdings jederzeit Nachweise verlangen. Es gibt

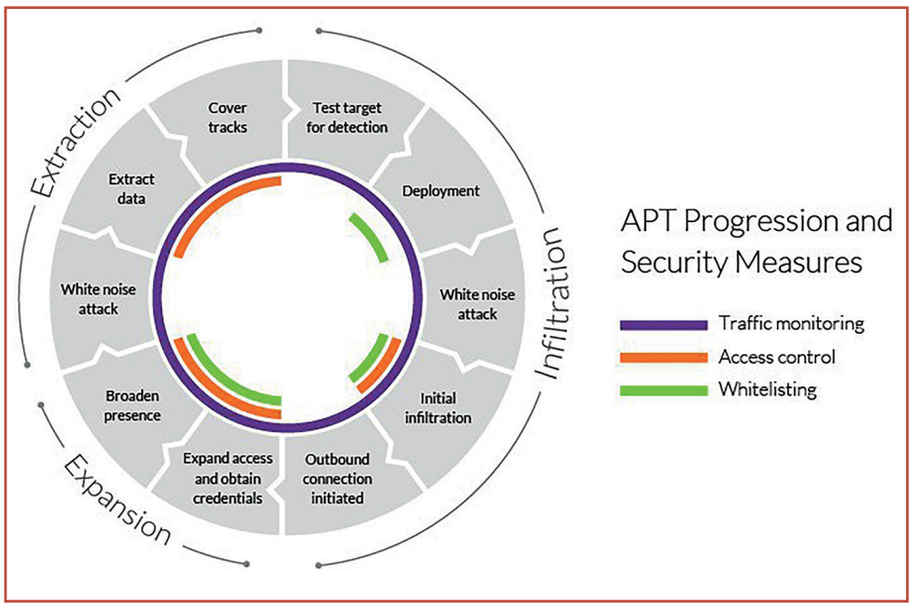


*Bild 2: SIEM-Systeme sind in der Lage, Advanced Persistent Threat (APT) Angriffe zu erkennen, die darauf ausgelegt sind, über einen längeren Zeitraum hinweg unbemerkt im Zielsystem zu bleiben, um Schwachstellen auszukundschaften (Grafik: Detken)*

aber auch bei NIS 2 eine Ausnahme von der Regel: Im ITK-Bereich sind auch kleinere Unternehmen betroffen, wenn sie DNS-Dienste oder Vertrauensdienste mit qualifiziertem Signaturmanagement anbieten. Diese Dienste gelten als sehr kritisch und unterliegen daher ebenfalls den NIS 2-Richtlinien.

## Organisatorische Maßnahmen

Die zehn Maßnahmen des NIS 2-Katalogs müssen von allen betroffenen Institutionen als Basisanforderung umgesetzt werden, denn sie werden für deutsches Recht direkt übernommen. Dabei bleiben die technisch notwendigen Maßnahmen abstrakt. Welche technischen Systeme verwendet werden sollen, um beispielsweise Zugriffskontrolle oder Bewältigung von Sicherheitsvorfällen zu ermöglichen, wird nicht beschrieben. Die NIS 2-Richtlinie verlangt, dass Konzepte und Verfahren zur Risikoanalyse vorhanden sind und dass das Unternehmen bewerten kann, wie wirksam diese Maßnahmen des Risikomanagements zur Stärkung der IT-Sicherheit sind. Auch muss die Bewältigung von Sicherheitsmaßnahmen zur Aufrechterhaltung oder Wiederherstellung des Betriebes nachgewiesen werden können. Dabei wird erstmals auch die Lieferkette mit einbezogen. Die NIS 2-Regelung setzt dazu die Implementierung eines Informationssicherheitssystems (ISMS) voraus. Dies ist ein systematischer Ansatz zur Verwaltung, Kontrolle und zum Schutz von sensiblen Informationen in einer Organisation. Ein ISMS umfasst Richtlinien, Verfahren, Prozesse und Technologien, die darauf abzielen, die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sicherzustellen. Ein ISMS ermöglicht es einer Organisation, Risiken zu identifizieren, zu bewerten und angemessene Kontrollen zu implementieren, um diese Risiken zu minimieren oder zu akzeptieren. Durch regelmäßige Überwachung, Bewertung und kontinuierliche Verbesserung hilft ein ISMS dabei, die Informationssicherheit auf einem angemessenen Niveau zu halten und sich an sich ändernde Bedrohungen und Anforderungen anzupassen.

Ein ISMS ist allerdings nur die eine Seite der Medaille. Denn damit sind noch nicht die notwendigen technischen IT-Systeme implementiert worden. Die Regularien verpflichten zwar die betrof-

fenen Unternehmen zur Einhaltung des „Stands der Technik“ bei der Absicherung der IT-Systeme und Netzwerke. Aber wie dies im Detail auszusehen hat, bleibt unbeschrieben. Eine Definition wäre auch problematisch, da der Stand der Technik sich kontinuierlich weiterentwickelt und neue Bedrohungen auftauchen. Es ist daher wichtig für Unternehmen, sich über aktuelle Trends und „Best Practises“ auf dem Laufenden zu halten und ihre Sicherheitsstrategien entsprechend anzupassen. Folgende Schlüsselbereiche lassen sich für den Stand der Technik nennen:

- Verschlüsselung: Die Verschlüsselung von Daten und Kommunikation über Netzwerke ist ein grundlegender Aspekt der IT-Sicherheit.
- Authentifizierung und Zugriffskontrolle: Die Implementierung von starken Authentifizierungsmethoden (Mehrfaktor-Authentifizierung) und das Verwalten von Zugriffsrechten und -berechtigungen verhindern den unberechtigten Zugriff auf firmeninterne Informationen.
- Sicherheitsüberwachung und -management: Netzwerke, Systeme und Anwendungen müssen kontinuierlich auf verdächtige Aktivitäten überwacht werden. Dazu ist die Implementierung eines SIEM-Systems vorzusehen.
- Patch-Management: Software und Systeme sind regelmäßig zu aktualisieren, um Sicherheitslücken zu schließen und die Angriffsfläche zu minimieren.
- Awareness und Schulung: Mitarbeiter müssen regelmäßig geschult werden, um das Sicherheitsbewusstsein zu stärken. Dadurch lassen sich Social-Engineering-Angriffe und interne Sicherheitsrisiken minimieren.
- Cloud-Sicherheit: Absicherung der Cloud-Dienste durch zusätzliche Sicherheitsmaßnahmen.
- Compliance und Datenschutz: Einhaltung von Datenschutzbestimmungen und Industriestandards wie der DSGVO und der ISO/IEC 27001 zur Erfüllung gesetzlicher Anforderungen und Schaffung von Kundenvertrauen.

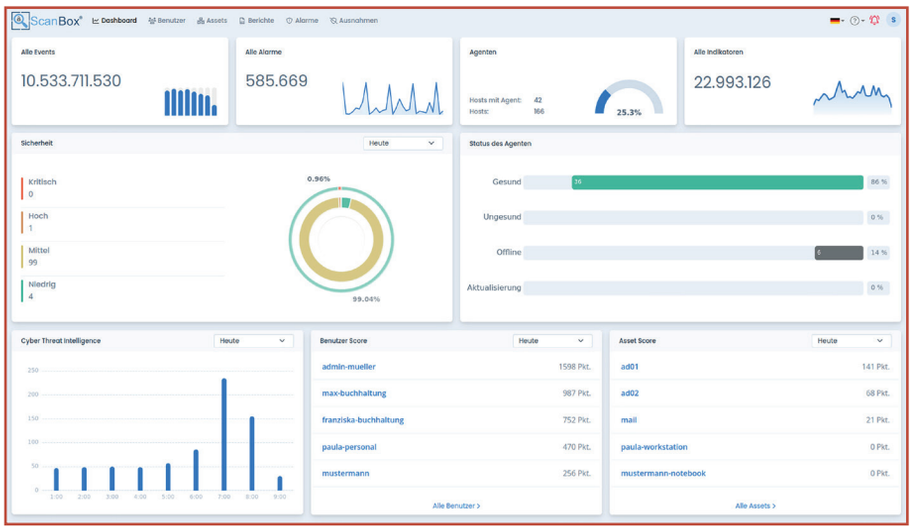


*Bild 3: Exemplarisches Dashboard der SIEM-Lösung ScanBox. Integrierte KI-Methoden erlauben es der Lösung, eine Verhaltensanalyse durchzuführen, um das normale Verhalten von Benutzern von ungewöhnlichen Vorfällen zu trennen (Bild: Detken)*

Die zentrale Sicherheitslösung in diesem Zusammenhang ist die Einführung eines SIEM-Systems, welches auch in der Lage ist, Advanced Persistent Threat (APT) Angriffe zu erkennen, die darauf ausgelegt sind, über einen längeren Zeitraum hinweg unbemerkt im Zielsystem zu bleiben, um Schwachstellen auskundschaften zu können (siehe Abbildung 2). Solche Angriffe sind schwer zu erkennen, da sie keinen unmittelbaren Alarm auslösen.

Dies sollte hingegen durch SIEM-Systeme mit integrierten KI-Methoden gelingen (siehe Abbildung 3). Denn diese ermöglichen, eine Verhaltensanalyse durchzuführen, um das normale Verhalten von Benutzern, Geräten und Anwendungen in einem Netzwerk von ungewöhnlichen Vorfällen (Incidents) zu trennen. Dies gelingt, indem nicht nur die Netzwerkdaten analysiert, sondern auch die Logging-Daten von Serversystemen geprüft und miteinander kombiniert (korreliert) werden. So lassen sich auch bisher unbekannte Bedrohungen erkennen und abwehren.

## Fazit

Ein SIEM-System in ein bestehendes Unternehmensnetz einzuführen, ist allerdings nicht trivial und kann je nach Umgebung einige Monate in Anspruch nehmen. Denn es müssen die IT-Systeme benannt werden, die es zu schützen gilt, und Regelwerke definiert bzw. das Normalverhalten ermittelt werden. Asset-Listen mit allen technischen Systemen müssten daher vorliegen. Diese fehlen aber in den meisten Unternehmen. Zwar ist mit Bußgeldern bei Nichteinhaltung frühestens in drei Jahren zu rechnen. Trotzdem sollte man sich auf die Einhaltung dieser neuen Regularien frühzeitig einstellen, da ihre Umsetzung grundlegend geplant werden sollte. Abschließend sei darauf hingewiesen, dass NIS 2 auch nicht alleine durch ein SIEM-System umgesetzt werden kann. Denn es ist ein ganzheitliches Risikomanagement gefordert, welches technische, operative und organisatorische Maßnahmen zur IT-Sicherheit bündelt. Ein wichtiger grundlegender Schritt auf der technischen Seite ist durch die SIEM-Einführung aber in jedem Fall getan. Danach müssen die organisatorischen Maßnahmen folgen, um zeitnah Meldungen und Berichte von Sicherheitsvorfällen dem BSI vorlegen zu können.