Verlagsbeilage, April 2025

Special
NIS-2
Sanktionen und Lösungen

kes
Die Zeitschrift für Informations-Sicherheit

Impressum

DATAKONTEXT GmbH

Augustinusstraße 11 A
50226 Frechen (DE)
Tel.: +49 2234 98949–30,
redaktion@datakontext.com,
www.datakontext.com

Geschäftsführer: Dr. Karl Ulrich

Handelsregister:
Amtsgericht Köln, HRB 82299

Anzeigenleitung: Birgit Eckert
(verantwortlich für den Anzeigenteil)
Tel.: +49 6728 289003, anzeigen@kes.de

Satz: Dirk Hemke (SatzPro), Krefeld;
Markus Miller (Satz+Bild), München

Druck: QUBUS media GmbH,
Beckstraße 10, 30457 Hannover

Bild: Adobe Stock/ImageKing

30 000 Unternehmen und Behörden betroffen

NIS-2: Härtere Vorgaben, strengere Regeln – auch für IT-Dienstleister

Mit der Network-and-Information-Security-Richtlinie 2.0 (NIS-2) hat die Europäische Union (EU) die Anforderungen an die IT-Sicherheit deutlich ausgeweitet. Sie erfasst nun rund 30.000 Unternehmen und öffentliche Einrichtungen. Obendrein müssen sich Organisationen, für die bereits NIS-1 und das IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0) gelten, auf schärfere Kontrollen, strengere Nachweispflichten sowie deutlich höhere Sanktionen einstellen. Das betrifft auch IT-Dienstleister und Rechenzentren.

Von Ina Märzluft, noris network AG

Mit NIS-2 verdeutlicht der europäische Gesetzgeber, dass er künftig keine Nachlässigkeit mehr im Umgang mit der Cybersicherheit und der Prävention von Online-Kriminalität dulden wird. So werden betroffene Unternehmen und Einrichtungen der öffentlichen Hand nach NIS-2-Lesart unter anderem fest dazu verpflichtet, robuste Sicherheitskonzepte zu implementieren. Sie umfassen sowohl technische als auch organisatorische Maßnahmen und haben zum Ziel, Netz- und Informationssysteme bestmöglich zu schützen. Ein besonderes Auge wirft die EU auf kritische Infrastrukturen (KRITIS) und Finanzinstitute. Sie sind dazu angehalten, umfassende Strategien zur Risikominimierung zu entwickeln und zeitnah umzusetzen.

Dazu gehören unter anderem die Analyse und Bewertung potenzieller Bedrohungen und deren Verhinderung, beispielsweise durch die Einführung von Intrusion-Detection- und Prevention-Systemen sowie starken Authentifizierungs- und Autorisierungskonzepten. Hier haben sich Multifaktor-Authentifizierung (MFA) und Zero-Trust-Architekturen (ZTA) beziehungsweise biometrische Verfahren durchgesetzt. Ebenso sind Notfallpläne für Disaster-Recovery und Business-Continuity mit Risikoanalysen und Hochverfügbarkeitsstrategien – Stichwort Georedundanz – künftig essenziell, um im Krisenfall schnell reagieren zu können. Auch proaktive Maßnahmen wie regelmäßige Penetrationstests und ein professionelles Schwachstellenmanagement spielen eine entscheidende Rolle, um Risiken zu minimieren und den Schutz der IT-Systeme weiter zu optimieren. Ebenso sind Incident-Response-Pläne sowie regelmäßige Schulungen für Mitarbeitende in der NIS-2-Novelle nicht mehr optional: Durch gezielte Trainings und Sensibilisierungsmaßnahmen für Mitarbeitende hofft die EU, wachsende Cybergefahren und Sicherheitslücken möglichst im Keim zu ersticken.

Strenge Audit-Pflichten für Unternehmen

Um die Sicherstellung der Einhaltung und die Wirksamkeit des Risikomanagements zu gewährleisten, sieht die NIS-2 Audits als wesentliche Bestandteile vor. Sie dienen dazu, Prozesse, Systeme und Organisationen systematisch und regelmäßig zu überprüfen und zu bewerten. Unternehmen müssen innerhalb dieser Audits nachweisen, dass sie die gesetzlichen Anforderungen der Direktive erfüllen. Dies betrifft besonders KRITIS-Betreiber, die gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI) dokumentieren müssen, dass ihre IT-Sicherheitsmaßnahmen tatsächlich den NIS-2-Vorschriften entsprechen.

Auditpflichten umfassen sowohl regelmäßige externe und interne Sicherheitsprüfungen zur Erkennung von Schwachstellen als auch umfassende Berichtspflichten gegenüber Aufsichtsbehörden über die Wirksamkeit der Sicherheitsmaßnahmen. Zudem sind Unternehmen und Behörden verpflichtet, alle sicherheitsrelevanten Prozesse und Vorfälle lückenlos zu dokumentieren. Banken und Finanzmarktinfrastrukturen sind dabei zusätzlich an die

Anforderungen der Europäischen Bankenaufsicht (EBA) gebunden; sie verzahnt NIS2-konforme Sicherheitsmaßnahmen eng mit den bestehenden IT-Governance-Richtlinien.

NIS-2 umfasst neue Branchen

NIS-2 teilt jetzt auch kleinere Unternehmen in „sehr kritische“ sowie „kritische Sektoren“ ein. Betroffen sind jetzt auch neue Branchensegmente wie Hersteller chemischer Stoffe, Produzenten medizinischer Geräte, Betriebe aus dem Segment der Lebensmittelverarbeitung und Organisationen, die Dienste für soziale Netzwerke bereitstellen. Allerdings gilt die NIS-2-Richtlinie vorerst nur für Einrichtungen, die wesentliche oder wichtige Dienste anbieten, besonders jene mit mindestens 50 Mitarbeitenden beziehungsweise einem Jahresumsatz ab zehn Millionen Euro.

Verschärfte Meldepflichten bei Sicherheitsvorfällen

Im Rahmen der Meldepflichten stehen Unternehmen laut NIS-2 in der Pflicht, „erhebliche Sicherheitsvorfälle“ innerhalb von 24 Stunden an das zuständige Computer-Security-Incident-Response-Team (CSIRT) oder eine nationale Behörde zu melden. Zusätzliche Berichte sind innerhalb von 72 Stunden sowie nach maximal einem Monat erforderlich. Ein erheblicher Sicherheitsvorfall liegt vor, wenn kritische Systeme betroffen, finanzielle oder betriebliche Auswirkungen erheblich sind oder Datenlecks beziehungsweise Datenschutzverstöße eintreten. Die frühzeitige Identifikation von Bedrohungen durch umfassende Monitoring-Systeme ist daher essenziell.

Zertifizierungen als Nachweis der IT-Sicherheit

Ein zentraler Aspekt der NIS-2-Umsetzung ist der Nachweis durch anerkannte Zertifizierungen. Sie bestätigen, dass Unternehmen die notwendigen Sicherheitsstandards einhalten. Besonders für KRITIS-Unternehmen und Finanzdienstleister spielen Standards wie ISO 27001, der BSI-Grundschutz sowie TÜViT TSI Level 4 eine wichtige Rolle. ISO 27001 bildet die Basis für ein wirksames Informationssicherheits-Managementsystem, während der BSI-Grundschutz als umfassendes Framework für IT-Sicherheit in Deutschland dient. Das TÜViT TSI Level 4-Zertifikat richtet sich besonders an Rechenzentren und bestätigt, dass höchste Sicherheitsanforderungen erfüllt werden. Dazu gehören unter anderem der Brandschutz und das Notfallmanagement für den Katastrophenfall. Außerdem stellen Zertifizierungen sicher, dass kritische Infrastrukturkomponenten wie Stromversorgung, Klimatisierung und Netzwerkverbindungen redundant und hochverfügbar zur Verfügung stehen. Finanzdienstleister und Betreiber kritischer Infrastrukturen profitieren von der Implementierung dieser Standards, da sie nicht nur Compliance-Anforderungen erfüllen, sondern auch das Vertrauen von Kunden und Partnern stärken. Vor allem für Banken und deren IT-Dienstleister haben sich Zertifizierungen längst zum entscheidenden Wettbewerbsfaktor entwickelt, da sie ihre Fähigkeit zur sicheren Verarbeitung sensibler Finanzdaten belegen.

NIS-2 setzt neue Standards in der Cybersicherheit

Klar ist: Mit der NIS-2-Richtlinie verschärft die EU die Anforderungen an Cybersicherheit erheblich. Besonders betroffen sind die Finanzbranche und KRITIS-Unternehmen – sowie ihre IT-Dienstleister und Rechenzentrumsbetreiber –, die umfassende Sicherheitskonzepte umsetzen, strenge Audit-Anforderungen erfüllen und anerkannte Zertifizierungen nachweisen müssen. Unternehmen, die sich rechtzeitig auf die neuen Vorgaben einstellen, sichern nicht nur ihre Compliance, sondern stärken auch ihre Widerstandsfähigkeit gegen Cyberangriffe. Unbestritten ist damit aber auch: Der Weg zur erfolgreichen Umsetzung von NIS-2 erfordert eine enge Zusammenarbeit zwischen IT-Sicherheitsverantwortlichen, Behörden und unabhängigen Prüfinstanzen, um höchste Sicherheitsstandards zu gewährleisten. Damit profitieren alle Beteiligten von der erhöhten Cybersicherheit, während das vorausschauende Sicherheitsmanagement zum Schlüssel für eine nachhaltige Resilienz gegenüber den Bedrohungen der digitalen Welt wird. ■

NIS-2 kompakt:

_____ Erweiterter Geltungsbereich: Gilt für mehr Sektoren und Unternehmen, darunter kritische und wichtige Einrichtungen.

_____ Strengere Cybersicherheitsmaßnahmen: Einführung von Risikomanagementmaßnahmen wie Incident Response, Verschlüsselung und Zugangskontrollen.

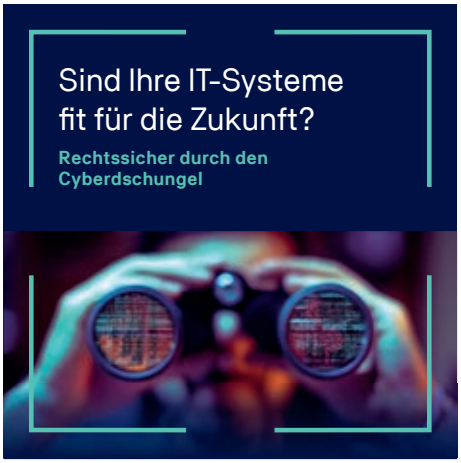
_____ Meldepflichten: Verpflichtung zur Meldung schwerwiegender Sicherheitsvorfälle innerhalb von 24 Stunden an die zuständige Behörde.

_____ Haftung und Sanktionen: Geschäftsleitung ist für Cybersicherheitsmaßnahmen verantwortlich; hohe Bußgelder bei Verstößen.

_____ Erhöhte Zusammenarbeit: Verbesserte Kommunikation und Informationsaustausch zwischen EU-Mitgliedstaaten und Unternehmen.

NIS-2: Die neue Superheldin der Cybersicherheit für Unternehmen

Aufgepasst, liebe Unternehmerinnen und Unternehmer!



Die Bedrohung im Cyberraum ist so hoch wie nie zuvor. Wussten Sie, dass laut einer Bitkom Umfrage[1] in 2024, 8 von 10 Unternehmen in Deutschland in den letzten 12 Monaten von Datendiebstahl, Spionage oder Sabotage betroffen waren? Die neue NIS-2-Richtlinie der EU ist die Antwort auf diese alarmierende Entwicklung.

Warum sollte Sie das interessieren?
Die NIS-2-Richtlinie betrifft nicht nur Großkonzerne, sondern auch kleine und mittlere Unternehmen (KMU). Sind Sie bereit für die neuen Anforderungen? Welche Maßnahmen müssen Sie ergreifen, um Ihre Cybersicherheit zu stärken? Und was passiert, wenn Sie die Vorgaben nicht einhalten?

Die Vorteile der NIS-2: Ein echter Game-Changer!

- **Erhöhte Sicherheit:** Schutz vor Cyberangriffen durch strenge Sicherheitsmaßnahmen.
- **Wettbewerbsvorteil:** Unternehmen, die die Richtlinie umsetzen, sichern sich einen Vorsprung.
- **Rechtliche Sicherheit:** Vermeidung von Bußgeldern und Reputationsverlusten.

[1] *Quelle: bitkom e.V.-Studie „Wirtschaftsschutz 2024“*

Die NIS-2-Richtlinie bringt mehrere wichtige Neuerungen mit sich, die jedes Unternehmen kennen sollte:

- **Geltungsbereich:** Sie betrifft jetzt mehr Branchen, zum Beispiel Lebensmittelproduzenten, Online-Marktplätze und Entsorgungsunternehmen.
- **Sicherheitsmaßnahmen:** Unternehmen müssen Schutzmaßnahmen einführen oder verbessern. Dazu gehören Risikoanalysen, Notfallpläne, Lieferkettensicherheit und Multi-Faktor-Authentifizierung.
- **Meldepflichten:** Organisationen melden Sicherheitsvorfälle innerhalb von 24 Stunden an das BSI. Eine erste Bewertung erfolgt innerhalb von 72 Stunden, ein Abschlussbericht innerhalb eines Monats.
- **Aufsicht:** Das BSI wird Aufsichtsbehörde und kann im Notfall die Geschäftsführung eines Unternehmens suspendieren.
- **Lieferkette:** Unternehmen müssen Risiken auch in ihrer Lieferkette managen. Das betrifft viele Zulieferer.
- **Schulungen:** Die Geschäftsführung muss sich in Cybersicherheit schulen lassen und Risiken managen.

Zeit zu handeln!
Nutzen Sie die Gelegenheit, sich umfassend zu informieren und vorzubereiten.

Hören Sie unseren Podcast „Wissen kompakt“ Episode:
Cybersicherheit ist Chefsache
NIS-2 im Fokus – Unwissenheit (bei der Cybersicherheit) schützt vor Strafe nicht.

www.tuev-nord.de/podcast-nis2

Ein Schutzschild für Ihr Business!
Mit unseren Weiterbildungen qualifizieren Sie sich oder Ihre Mitarbeiter für diese wichtigen Aufgaben und setzen die hohen Anforderungen der NIS-2-Richtlinie an Unternehmen sicher um.

Stellen Sie die Weichen für eine starke IT-Sicherheit in Ihrem Unternehmen!

Alle Details zu den **TÜV NORD Akademie** Seminaren zur **NIS2-Richtlinie**

Vertrauenswürdige IT-Sicherheit: Schlüssel zur digitalen Souveränität

Aktuelle geopolitische Entwicklungen machen klar: Nie war der Schutz digitaler Infrastrukturen und sensibler Daten wichtiger als heute. IT-Sicherheitsprodukte „Made in Germany" sind das Mittel der Wahl, um regulatorische Anforderungen zu erfüllen, Abhängigkeiten von ausländischen Anbietern zu reduzieren und die eigene digitale Souveränität zu stärken.

Von Arnold Krille, genua GmbH

Für Unternehmen und Behörden öffnet die fortschreitende Digitalisierung viele Chancen, gleichzeitig stresst sie die IT-Sicherheit: Mit jedem neuen Netzwerkanschluss wächst die potenzielle Angriffsfläche. Nicht zuletzt aufgrund aktueller geo- und sicherheitspolitischer Entwicklungen gewinnt daher das Thema digitale Souveränität schnell an Bedeutung.

Digitale Souveränität beschreibt die Fähigkeit von Organisationen, ihre digitalen Infrastrukturen und sensiblen Daten eigenständig zu kontrollieren, uneingeschränkt darüber verfügen zu können und sie vor externen Einflüssen und Bedrohungen zu schützen. Digitale Souveränität ist die Grundlage für die souveräne Erfüllung des Auftrags einer Organisation, sowohl bei Wirtschaftsunternehmen als auch bei staatlichen Institutionen. Abhängigkeiten von ausländischen IT-Anbietern können dabei zum Problem werden. Das ist besonders relevant angesichts zunehmender staatlicher und wirtschaftlicher Spionage. Auch die sich ändernden geopolitischen Bündnisse sorgen hier für Unsicherheiten und Risiken.

Vertrauenswürdige IT-Sicherheitsprodukte spielen in diesem Zusammenhang eine Schlüsselrolle. Die genua GmbH als deutscher Hersteller bietet mit ihren vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zugelassenen IT-Sicherheitslösungen essenzielle Bausteine, um regulatorische Anforderungen zu erfüllen und die eigene digitale Souveränität zu stärken.

NIS-2: Kritische Infrastrukturen schützen

Eine leistungsfähige, resiliente Cybersicherheit ist nicht nur für Einzelunternehmen wichtig. Sie ist ebenso unverzichtbar für das Funktionieren staatlicher und gesellschaftlicher Strukturen. Ein besonderes Augenmerk hat die Europäische Kommission daher auf kritische Infrastrukturen (KRITIS) gerichtet, die verbindliche Cybersicherheitsrichtlinie NIS-2 definiert und 2023 in Kraft gesetzt wurde. Die Mitgliedstaaten müssen diese Richtlinie in nationale Gesetze umsetzen. Auch in Deutschland wird es im Jahr 2025 zur verspäteten Umsetzung kommen. Die Vorgaben betreffen Unternehmen mit mindestens 50 Mitarbeitern und 10 Millionen Euro Jahresumsatz. In Deutschland fallen darunter somit schätzungsweise 30 000 Unternehmen aus den 18 KRITIS-Sektoren. Die NIS-2-Richtlinie verpflichtet diese Unternehmen, nachweislich angemessene Maßnahmen umzusetzen, welche die Sicherheit und Widerstandsfähigkeit der Netzwerke und Informationssysteme gewährleisten. Diese Maßnahmen umfassen Risikomanagement, technische und organisatorische Maßnahmen der Informationssicherheit, Meldung von Vorfällen sowie die Umsetzung von Business-Continuity-Maßnahmen.

Die genua GmbH bietet eine Reihe von Lösungen an, welche die Organisationen und Unternehmen bei der Umsetzung der NIS-2-Vorgaben unterstützen.

Eine der Vorgaben ist, ein System zur Angriffserkennung umzusetzen. Dafür eignet sich der cognitix Threat Defender: Er kombiniert ein Intrusion-Detection-System (IDS) mit einem Intrusion-Prevention-System (IPS) zu einer Komplettlösung, die den Datenverkehr und die Assets im Netzwerk nichtinvasiv analysiert, schnell Anomalien erkennt und dynamische gezielte Gegenmaßnahmen ermöglicht. Ferner beherrscht die intelligente IDS/IPS-Lösung die Mikrosegmentierung bis auf Anwendungsebene (Layer 7) und liefert wertvolle Netzwerkinformationen für forensische Analysen. Das Lösungs- und

Anomalie-Erkennung: cognitix Threat Defender erkennt den Traffic von über 3700 Anwendungen/ Apps und Protokollen in Echtzeit – und meldet zielsicher Anomalien. (Bild: genua)

Einsatzkonzept mit On-Premise-Betrieb sichert dem Anwender 100-prozentige Datenhoheit zu.

Gezielte Segmentierung

Ein weiterer Punkt zum Schutz kritischer Infrastrukturen ist die zuverlässige Trennung von internen und externen Kommunikationsnetzwerken. An der Nahtstelle zwischen Internet und lokalem Netzwerk sorgt die High Resistance Firewall genugate für ein Höchstmaß an Sicherheit. Die einzige vom BSI als „highly resistant" eingestufte Firewall der Welt erfüllt höchste Anforderungen: Zwei unterschiedliche Firewall-Systeme – ein Application-Level-Gateway und ein Paketfilter jeweils auf separater Hardware – sind zu einer kompakten Lösung kombiniert.

Mehr Sicherheit für Produktionsnetzwerke ergibt sich durch eine zuverlässige Segmentierung. Mit der Industrial Firewall genuwall lassen sich in Produktionsnetzen (LAN, WAN und VLANs) hochwirksame Barrieren gegen Angriffe aufbauen. Je nach Schutzbedarf werden für einzelne Maschinen, Anlagen oder ganze Produktionsbereiche getrennte Sicherheitszonen geschaffen. Für die Trennung sorgt genuwall. Die Firewall kontrolliert zuverlässig den gesamten Datenverkehr und lässt ausschließlich die gewünschten Verbindungen zu.

Mögliche Risiken bei der digitalen Vernetzung hochkritischer Steuerungssysteme lassen sich mit der Datendiode cyber-diode minimieren. Diese Lösung lässt ausschließlich Einbahn-Datentransfers zu – in Gegenrichtung wird dagegen jeder Informationsfluss konsequent geblockt. Geschützt hinter der cyber-diode können Maschinen, Anlagen und IT-Systeme somit Daten über öffentliche Netze versenden, ohne dass die Integrität der Maschine oder Maschinensteuerung gefährdet wird.

genubox kombiniert die Vorteile für sichere Fernwartung mit Privileged-Access-Management-Funktionen. Dazu zählen die Überwachung von Zugriffen auf kritische Ressourcen und die Abwehr unbefugter Handlungen im Netzwerk.

Hohes Schutzniveau

Angesichts der dynamischen geo- und sicherheitspolitischen Entwicklungen gewinnt die digitale Souveränität auch im Umfeld der geheimschutzbetreuten Industrie an Bedeutung. Schon vor den aktuellen geopolitischen Entwicklungen, aber unter dem Eindruck des russischen Angriffs auf die Ukraine, hat der Gesetzgeber die Anforderungen im Geheimschutz-Merkblatt des Bundesministeriums für Wirtschaft und Klimaschutz (BMWK) spürbar angehoben. Im VS-NfD-Merkblatt (GHB-Anlage 4) sind klare Anforderungen an den Schutz von Verschlusssachen des Geheimhaltungsgrades „VS – Nur für den Dienstgebrauch" (VS-NfD) formuliert. Die Frist zur Umsetzung der angepassten Anforderungen aus dem VS-NfD-Merkblatt endet am 1. September 2025.

Ist ein VS-NfD-Netzwerk mit Netzsegmenten verbunden, die ein niedrigeres Sicherheitsniveau haben, schreibt das Merkblatt zusätzliche Sicherungsmaßnahmen vor. An der kritischen Nahtstelle beispielsweise zwischen Internet und lokalem Netz soll demnach eine Trennung durch Firewalls in einer sogenannten P-A-P-Struktur (Paketfilter – Application Layer Gateway – Paketfilter) und die regelmäßige Überprüfung der Firewallregeln erfolgen. Durch die vorgelagerten Paketfilter wird das Application-Level-Gateway an beiden Seiten sowohl gegen direkte Angriffe als auch gegen hohe Belastungen optimal geschützt.

Mit der zweistufigen High-Resistance Firewall genugate von genua und einem weiteren Paketfilter lässt sich dieses hohe Sicherheitsniveau komfortabel erreichen: Sie kombiniert stateful-Paketfilter (PFL) und Application-Level-Gateway (ALG) in einer kompakten Lösung. genugate ist zertifiziert nach EAL4+ mit AVA.VAN.5, zudem schützt ein hochsicherer Update-Mechanismus vor Supply-Chain-Angriffen mit zukünftigen Quantencomputern.

Fazit

Vertrauenswürdige IT-Sicherheitslösungen bilden die Grundlage für das Erfüllen der NIS-2-Vorgaben, für den Aufbau VS-NfD-konformer IT-Infrastrukturen und letztlich für das Sicherstellen der geschäftlichen Leistungsfähigkeit durch digitale Souveränität.

Die genua GmbH, ein Unternehmen der Bundesdruckerei-Gruppe, entwickelt IT-Sicherheitslösungen nach höchsten Standards und etablierten Richtlinien wie Security by Design in Deutschland. genua begleitet KRITIS-Organisationen von der Konzeption einer rechtssicheren IT-Security-Infrastruktur über die Auswahl und Implementierung konformer IT-Sicherheitsprodukte bis hin zu Training und Vor-Ort-Support der internen Teams. ■

noris network

Ihr Premium-IT-Dienstleister für **zukunftssichere Cloud-Lösungen**

- **Maximale Sicherheit und Vertrauen:** Hochsichere, zertifizierte Rechenzentren in Deutschland
- **Flexibilität nach Maß:** Private, Public oder Hybrid Cloud – individuell anpassbar und hochverfügbar
- **Passgenaue Lösungen:** Vielfältige Cloud-Services für Ihre individuellen Anforderungen
- **Regelkonform und zuverlässig:** Expertenwissen für Governance, Compliance und Datenschutz
- **Transparente Kosten:** Keine versteckten Gebühren

Jetzt informieren

NIS-2 aktiv statt reaktiv umsetzen

Datenwäsche: Cyberangriffe stoppen, bevor sie starten

Die Cyberbedrohungslage in Deutschland verschärft sich kontinuierlich – darin sind sich alle Sicherheitsbehörden einig. Für von NIS-2 betroffene Unternehmen ist es kostengünstiger, IT-Risiken frühzeitig zu vermeiden, als später aufwendige Meldungen und Krisenmanagement zu betreiben. Präventive Maßnahmen werden daher immer wichtiger.

Von Ramon Mörl, itWatch GmbH

Jeder Angriff erfordert ein Stückchen Code, der sich in Daten oder ausführbaren Elementen verbirgt – sei es in Downloads, E-Mails, mobilen Datenträgern, der Firmware angeschlossener Hardware oder sogar in Software-Patches. Es gibt zahlreiche Einfallstore. Daten aus der Personalabteilung (etwa Bewerbungen), dem Vertrieb, dem Kundenservice, dem Marketing oder der Technik sind nicht zwangsläufig so vertrauenswürdig wie interne Unternehmensdaten. Bevor solche Daten intern genutzt werden können, müssen sie überprüft und gesäubert werden. Eine einfache Antivirenprüfung genügt nicht, da selbst infizierte Dateien wertvolle Informationen oder Bewerbungen für die Personalabteilung enthalten können – schließlich schützt nicht jeder Bewerber sein Smartphone ausreichend. Dieser Prozess wird als Datenwäsche bezeichnet.

Durch das Öffnen einer Bilddatei im JPG-Format oder eines PDF-Dokuments kann etwa ein Skript geladen werden, das die Konfiguration des Remote-Desktop-Tools so verändert, dass Unbefugte die Rechte des Mitarbeiters übernehmen können. Schädlich, aber kein bekannter Schadcode. Auch verschlüsselte Daten in Archiven wie ZIP und anderen Formaten oder in beliebigen anderen Dateien können schädliche Objekte bis auf die Clients und Server transportieren – und entgehen dabei gängigen Schutzmechanismen. Bekannte Viren können von Antivirenscannern (AV) nicht erkannt und neutralisiert werden, wenn sie in einer verschlüsselten Datei oder in tief verschachtelten Archiven eingebettet sind.

Schadsoftware, die zum Beispiel versteckt in verschlüsselten E-Mail-Anhängen unbemerkt ins Unternehmen gelangt und sich im gesamten betriebsinternen System ausbreitet, bedroht die eigene kritische IT erheblich. Kritisch ist natürlich auch das Ausbreiten von Schadcode in den Produkten eines Unternehmens, da die gesamte weitere Lieferkette betroffen ist und zudem ein nicht zu

Bild: itWatch/iStock.com

unterschätzendes und oft unklares Haftungsrisiko entsteht. Für KRITIS-Organisationen ist deshalb auch die Prüfung zugelieferter Software- und Hardwareprodukte wesentlich. Leicht kann in einem Rauchmelder, einer Überwachungskamera oder anderen Geräten zusätzliche Funktionalität wie Wi-Fi, Mikrofon und Kamera untergebracht sein und so auch in nicht vernetzten Geräten eine Bedrohung entstehen.

Cybersicherheit als Enabler

In den oben beschriebenen Szenarien ist „Nicht anklicken, nicht öffnen, nicht nutzen“ keine Option! Die kritischen Leistungen und Services müssen in NIS-2 regulierten Organisationen – trotz möglicher Angriffe – erbracht und die damit verbundenen Arbeiten weiter erledigt werden. Dazu muss die IT für diese Arbeiten funktionieren. Eine Netztrennung zwischen kritischen IT-Elementen und weniger sensibler Infrastruktur schützt die KRITIS-Elemente, addiert aber Komplexität und wird oft – wie viele präventive Sicherheitsmaßnahmen – vom Anwender als hinderlich wahrgenommen. Das Problem wird durch eine netztrennende Schleuse mit Datenwäsche

und Workflow nach einem patentierten Verfahren gelöst (itWash.de). Diese netztrennende Datenschleuse ist auch gegenüber dem Internet bezüglich E-Mails aus unsicheren Domänen, Downloads oder Datentransportverfahren wie OneDrive, WeTransfer, S-FTP nutzbar.

Jeder unbekannte Code im Datenzufluss von extern nach intern wird identifiziert. Datenobjekte dürfen nur bekannte oder vertrauenswürdige Codeelemente enthalten – signierte Skripte, Makros oder solche, die in einer Whitelist mit ihren authentisierenden Eigenschaften hinterlegt sind.

Eingehender Code, also neue Software, Patches et cetera, wird nur von einem vertrauenswürdigen Kanal übernommen und in seine Bestandteile zerlegt, indem eine Software Bill of Material (SBOM) erstellt wird. Zu jedem Element werden die Verletzbarkeiten (Common Vulnerabilities and Exposures, CVE) ermittelt und für das Lifecyclemanagement hinterlegt. Die Betriebssystemhärtung durch die itWatch Enterprise Security Suite (itWESS.de) übernimmt die freigegebenen Softwareelemente in ihre Whitelist. Die CVEs werden zyklisch neu geprüft und bei definierten Schwellwerten geeignet reagiert (Alert oder Sperre).

Datenwäsche mit passendem Waschpulver

Die Datenwäsche besteht darin, die Daten in ihre Einzelteile zu zerlegen und jedes einzelne Element rekursiv einzeln erneut der Wäsche zuzuführen. Für jeden Datentyp wird automatisch das richtige Waschprogramm und Waschpulver gewählt. Danach werden die sauberen, also von allem Schmutz befreiten Daten, wieder zusammengesetzt und der Anwender erhält einen Bericht, ob und was verändert wurde. Schmutzige Elemente werden zur Beweissicherung gespeichert – natürlich verschlüsselt, damit sie nicht „ausbrechen“ können.

Die Voraussetzung für eine Wäsche ist, dass die Daten im Klartext vorliegen – denn eine Wäsche in einer wasserdicht verschlossenen Verpackung würde auch in der analogen Welt keinen Sinn ergeben. itWash verfügt deshalb über eine Erkennung von verschlüsselten Objekten und führt diese vor der Wäsche der Entschlüsselung durch den Anwender zu, ohne dass dessen Betriebssystem auf die Daten zugreifen kann.

Ein wesentlicher Vorteil gegenüber anderen Verfahren ist, dass jeder Bestandteil rekursiv zerlegt wird und jedes einzelne entstehende Objekt erneut allen Prüfungen – Verschlüsselung, Antivirus, Dateitypenauthentisierung, Inhaltsprüfung et cetera – unterzogen wird. Hierbei werden Verschlüsselungen und Modifikationen sicher erkannt und berücksichtigt. Insofern sind die in itWash angewendeten Verfahren deutlich mächtiger als die unter Content Disarm and Recover (CDR) vermarkteten Lösungen und können genauso auf dem Weg „nach draußen“ als Data Loss Prevention (DLP) eingesetzt werden.

Während der Wäsche werden automatisch Informationen zur richtigen Behandlung gewonnen – darunter der Einlieferer, die Herkunft sowie enthaltene Metadaten wie Geolokationen, Zeitstempel, erkannte Objekte in Bildern oder transkribierter Text aus Sprachdateien (Voice2Text). Diese Daten bestimmen das passende „Waschmittel“, die gewünschte Standardisierung (z. B. Konvertierung von Mediendaten in MP3 oder MP4) und das Ziel, an das die bereinigten Daten weitergeleitet werden sollen. Ein Algorithmus ermittelt das Übertragungsziel, setzt dort die passenden Zugriffsrechte und wendet bei Bedarf die geeignete Verschlüsselung an.

Wenn die eigene IT nicht verändert werden soll oder darf, ist eine Wäsche auch als Service in der Cloud oder in einem Rechenzentrum möglich (siehe Testbeispiel unten). Datenwäsche als mandantenfähiger Managed Service, der sowohl die Datenschutz-Grundverordnung (DSGVO) als auch branchenspezifische Regulierungen erfüllt, kann ganze Unternehmensverbünde und Lieferketten absichern. Weitere Informationen dazu finden Sie im Artikel „Datenwäsche als Cloud-Service“ im <kes>-Special 06/2024.

Security „Made in Germany“

itWatch ist einer der wenigen inhabergeführten Cybersecurity-Hersteller in Deutschland und entwickelt patentierte IT-Sicherheitslösungen „Made in Germany“. Die Enterprise Security Suite (itWESS) und die Datenschleuse (itWash) schützen Tausende als GEHEIM klassifizierte IT-Umgebungen, die auf der Skala der Common-Criteria-Prüfungen höher als eine CC EAL 4+-Prüfung zu bewerten sind, da nicht nur anhand eines herstellerdefinierten Protection-Profiles geprüft wird. Stattdessen werden alle Facetten der Produkte in realen, vernetzten Einsatzumgebungen getestet und durch professionelle Pentester verschiedenen Angriffsszenarien ausgesetzt. ■

genua ist made in Germany – für Ihre digitale Souveränität.

Teil der Bundesdruckerei-Gruppe

bdr.

Kritische Infrastrukturen wirksam schützen.

Excellence in Digital Security.

Rüsten Sie sich für das IT-Sicherheitsgesetz und NIS 2 mit Lösungen von genua. Secure by Design, KRITIS-spezifisch und gemäß BSI-Empfehlung schützen wir Ihre Energieinfrastrukturen umfassend vor Cyberangriffen. Anlagen- und Netzwerkschutz durch hochsichere Zero-Trust-Fernwartung, One-way-Datenübertragung für Predictive Maintenance sowie Anomalie-Erkennung.

Vertrauen Sie auf genua – für sichere und robuste IT-Infrastrukturen.

genua.

Sicherheitsstrategie im Wandel:

Wer erst reagiert, hat schon verloren

Durchdachte Sicherheitskonzepte und innovative Ansätze erhöhen die Widerstandsfähigkeit von Unternehmen gegenüber Cyberbedrohungen. Der entscheidende Fortschritt liegt in der Abkehr von rein reaktiven Maßnahmen hin zu einer proaktiven Strategie, die Angriffe erkennt und abwehrt, bevor sie Schaden anrichten können. Von diesem Wandel profitieren alle, nicht nur NIS-2-Organisationen.

Von Michael Klatte, ESET Deutschland GmbH

Unternehmen investieren weltweit massiv in Cybersecurity – und doch steigen die Schäden durch Cyberangriffe weiter. Laut der Studie „Wirtschaftsschutz 2024" des Digitalverbands Bitkom beliefen sich die finanziellen Verluste durch Cyberkriminalität im vergangenen Jahr auf 267 Milliarden Euro, ein Anstieg von 29 Prozent. 81 Prozent der Unternehmen berichteten von Angriffen in Form von Diebstahl, Industriespionage oder Sabotage. Diese Zahlen werfen eine entscheidende Frage auf: Warum führen höhere Investitionen nicht zu besserem Schutz? Ist sogar die NIS-2-Compliance in Gefahr?

Der Grund liegt in veralteten Sicherheitsansätzen. Viele Unternehmen setzen immer noch auf reaktive Schutzmaßnahmen, die erst eingreifen, wenn der Schaden bereits entstanden ist. Gleichzeitig sind Cyberkriminelle schneller, professioneller und nutzen zunehmend auf künstliche Intelligenz (KI) basierte Angriffsmethoden. Die Konsequenz? Unternehmen müssen ihre Strategie überdenken und den Fokus auf proaktive Sicherheitskonzepte legen, um Bedrohungen bereits im Vorfeld abzuwehren.

Warum klassische Sicherheitslösungen nicht mehr ausreichen

Die IT-Sicherheit vieler Unternehmen basiert auf traditionellen Maßnahmen wie Firewalls oder Antivirenprogrammen. Diese Werkzeuge sind zwar wichtig, aber sie allein reichen längst nicht mehr aus. Ein wesentlicher Schwachpunkt ist die fehlende frühzeitige Bedrohungserkennung. Angreifer können unbemerkt monatelang Netzwerke infiltrieren, bevor der eigentliche Angriff erfolgt. Zudem spielen die Herkunft und die Vertrauenswürdigkeit der eingesetzten Sicherheitssoftware eine entscheidende Rolle.

Ein oft übersehenes Risiko ist die Abhängigkeit von Anbietern, die aus Ländern mit fragwürdigen Datenschutzrichtlinien stammen. Die Diskussion um den sogenannten „Kill Switch" – also die Möglichkeit, dass Hersteller aus Drittstaaten ihre Sicherheitslösungen aus der Ferne deaktivieren können – zeigt die Dringlichkeit, auf vertrauenswürdige europäische Anbieter zu setzen. Sicherheitsunternehmen aus der Europäischen Union, wie ESET, garantieren hohe Datenschutzstandards und entsprechen strengsten Compliance-Anforderungen. Sie bieten transparente, technologisch führende Lösungen ohne versteckte Hintertüren, gewährleisten den Stand der Technik und verhelfen zur NIS-2-Compliance.

„Prevention First"

Vorbeugen statt heilen – was in der Medizin gilt, muss auch für Cybersecurity zum Standard werden. Proaktive Sicherheitsstrategien setzen genau hier an: Bedrohungen frühzeitig erkennen, Sicherheitslücken schließen und Angriffe verhindern, bevor sie entstehen. Dazu gehören essenzielle Maßnahmen:

- Patch-Management: Software-Schwachstellen schnell schließen, bevor Angreifer sie ausnutzen können.
- Multi-Faktor-Authentifizierung (MFA): Effektiver Schutz vor unbefugtem Zugriff durch zusätzliche Sicherheitsebenen.

_____ Endpoint Detection and Response (EDR): Kontinuierliche Überwachung von Endgeräten, um Anomalien frühzeitig zu erkennen.

Trotz der Verfügbarkeit dieser bewährten Methoden setzen viele Unternehmen weiterhin auf eine rein reaktive IT-Sicherheitsstrategie – eine gefährliche Fehleinschätzung.

Prävention mit fachkundiger Hilfe

Laut einer Umfrage von Cybersecurity Insiders aus dem Jahr 2023 haben 70 Prozent der IT-Experten Schwierigkeiten, Sicherheitslösungen effektiv zu implementieren und zu nutzen. Die zunehmende Komplexität der IT-Landschaft und der Fachkräftemangel verstärken dieses Problem. Die Lösung: Security-Services von spezialisierten Anbietern, die Unternehmen dabei unterstützen, ihre Sicherheitsarchitektur maßgeschneidert zu optimieren.

Anstatt komplexe Systeme in Eigenregie zu implementieren, empfiehlt sich die Zusammenarbeit mit Experten. Unternehmen wie ESET bieten umfassende Security-Services an, die über die bloße Bereitstellung von Software hinausgehen. Denn sie verfolgen den Ansatz des „Prevention first“: Sicherheitslücken schließen, Bedrohungen frühzeitig erkennen und neutralisieren, statt nur auf sie zu reagieren. ESET adressiert diese Herausforderungen mit einem umfassenden Portfolio unterschiedlicher Security-Services. Diese Dienstleistungen bieten Unternehmen Zugang zu Expertenwissen auf Wunsch und ermöglichen eine kontinuierliche Optimierung ihrer Sicherheitslösungen. Ferner unterstützen sie bei der proaktiven Gefahrenabwehr und entlasten interne Ressourcen. Beispiele dafür sind *ESET Premium Support / Ultimate* oder *ESET Threat Intelligence.*

MDR: Die Zukunft der Cyberabwehr

Eine besonders effiziente Lösung, um Cyberbedrohungen frühzeitig zu stoppen, ist Managed Detection and Response (MDR). Dabei übergeben Unternehmen ihre IT-Sicherheitsüberwachung an erfahrene, externe Dienstleister. MDR bietet rund um die Uhr Schutz, kombiniert mit KI-gestützter Analyse, um Bedrohungen in Echtzeit zu erkennen und zu stoppen. ESET MDR übernimmt zum Beispiel:

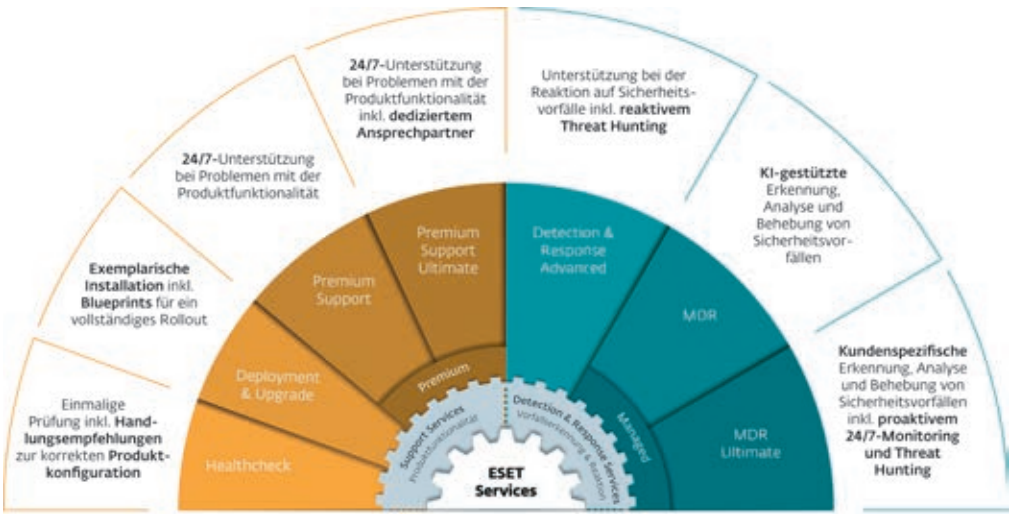
_____ 24/7-Systemüberwachung und Bedrohungserkennung
_____ automatisierte Reaktion auf Sicherheitsvorfälle
_____ KI-gestützte Analyse zur Abwehr hoch entwickelter Angriffe

Dank einer Verbindung mit dem ESET-eigenen Security-Information-and-Event-Management-(SIEM)-Tool können Bedrohungen innerhalb von 20 Minuten erkannt und gestoppt werden. Unternehmen profitieren dabei von einer Kombination aus aktueller Technologie und menschlicher Expertise – ein entscheidender Vorteil im Kampf gegen Cyberkriminalität.

Fazit

Die Zeiten rein reaktiver IT-Sicherheitsmaßnahmen sind vorbei. Unternehmen, die sich weiterhin nur auf klassische Schutzmechanismen verlassen, setzen ihre Systeme und Daten einem unnötigen Risiko aus. Der Schlüssel liegt in einer proaktiven Sicherheitsstrategie, die auf Prävention, kontinuierliche Überwachung und KI-gestützte Abwehrmechanismen setzt.

Mit Managed Detection and Response, KI-gestützter Bedrohungserkennung und professionellen Security-Services können Unternehmen ihre Cyberresilienz deutlich verbessern – und gleichzeitig Compliance-Anforderungen wie NIS-2 erfüllen. Europäische Sicherheitsanbieter wie ESET stellen Lösungen bereit, die den höchsten Datenschutzstandards entsprechen und Unternehmen umfassenden Schutz bieten. ■



Die Services von ESET im Überblick. (Bild: ESET)

EU-Sicherheitsrichtlinie NIS-2: Verpflichtungen, Fristen und Risiken im Überblick

Die NIS-2-Richtlinie ist seit Januar 2025 für viele Unternehmen in Europa eine verbindliche Vorgabe. Die nationale Umsetzung in Deutschland verzögert sich jedoch. Das NIS2-Umsetzungsgesetz (NIS2UmsuCG) sollte ursprünglich bis zum 17. Oktober 2024 in Kraft treten, wurde jedoch aufgrund der politischen Lage und der anstehenden Regierungsbildung verschoben. Eine Verabschiedung wird frühestens im Sommer 2025 erwartet. Trotz dieser Verzögerung sollten Unternehmen bereits jetzt Maßnahmen ergreifen, da es keine Übergangsfrist gibt und die Anforderungen unmittelbar gelten, sobald das Gesetz verabschiedet wird.

Aktueller Stand der NIS-2-Umsetzung

Die NIS-2-Richtlinie bringt wesentliche Änderungen im Bereich der Cybersicherheit mit sich. Der Anwendungsbereich wurde erheblich ausgeweitet und umfasst neben den bisherigen KRITIS-Sektoren auch **IT-Dienstleister, digitale Plattformen, Cloud-Anbieter, Rechenzentren und Teile der Lieferkette**. Unternehmen müssen strengere Sicherheitsvorgaben umsetzen und ihre Cyber-Resilienz verbessern. Eine zentrale Neuerung ist die **persönliche Haftung der Geschäftsführung**, die für die Einhaltung der Vorgaben verantwortlich ist.

Darüber hinaus sieht die Richtlinie **verschärfte Meldepflichten** vor. Sicherheitsvorfälle müssen innerhalb von **24 Stunden** gemeldet und anschließend detaillierte Berichte vorgelegt werden. Zudem sind umfassende **Risikomanagementmaßnahmen** erforderlich, um Schwachstellen in der IT-Infrastruktur zu identifizieren und proaktiv zu minimieren.

Konsequenzen bei Nichteinhaltung

Die Einhaltung der NIS-2-Richtlinie ist nicht nur eine rechtliche Verpflichtung, sondern entscheidend für die langfristige Sicherheit von Unternehmen. Verstöße gegen die Vorschriften können mit erheblichen Sanktionen geahndet werden. Vorgesehen sind **Bußgelder von bis zu 10 Millionen Euro oder 2 % des weltweiten Jahresumsatzes**.

Empfohlene Maßnahmen zur Vorbereitung

Auch wenn das nationale Umsetzungsgesetz noch aussteht, sind die Kernanforderungen bereits bekannt und sollten frühzeitig umgesetzt werden. Unternehmen sollten daher:

1. **Bestehende Sicherheitsstrukturen überprüfen und optimieren**, um den gestiegenen Anforderungen gerecht zu werden.
2. **Interne Meldeprozesse anpassen**, um sicherzustellen, dass Sicherheitsvorfälle fristgerecht gemeldet werden.
3. **Mitarbeitende und Geschäftsführungen sensibilisieren**, um ein besseres Verständnis für die neuen Pflichten und Maßnahmen zu schaffen.
4. **Lieferketten und Dienstleister einbeziehen**, da auch Drittanbieter höhere Sicherheitsstandards erfüllen müssen.

Fachliche Weiterbildung als zentrale Maßnahme

Eine erfolgreiche Umsetzung der NIS-2-Richtlinie erfordert umfassendes Fachwissen. Die **Bitkom Akademie** bietet spezialisierte **Seminare zur NIS-2-Richtlinie** an, die IT-Sicherheitsverantwortlichen, Datenschutzbeauftragten und Entscheidungsträgern praxisnahe und rechtssichere Handlungsempfehlungen vermitteln.

Haben Sie Fragen zu unseren Seminaren und dem Inhouse-Angebot im Bereich IT-Sicherheit? Dann kontaktieren Sie Vincent Bergner. ■

v.bergner@bitkom-service.de

bitkom akademie

Automatisierte Bedrohungserkennung mit ScanBox

Die Umsetzung der NIS-2-Richtlinie ist oft komplex und ressourcenintensiv. Die ScanBox von DECOIT bietet eine einfache, skalierbare Lösung zur Angriffserkennung. Sie erleichtert die Einhaltung der Vorgaben durch intelligente Analyse und Expertenunterstützung.

Von Michael Schulte, freier Redakteur in München

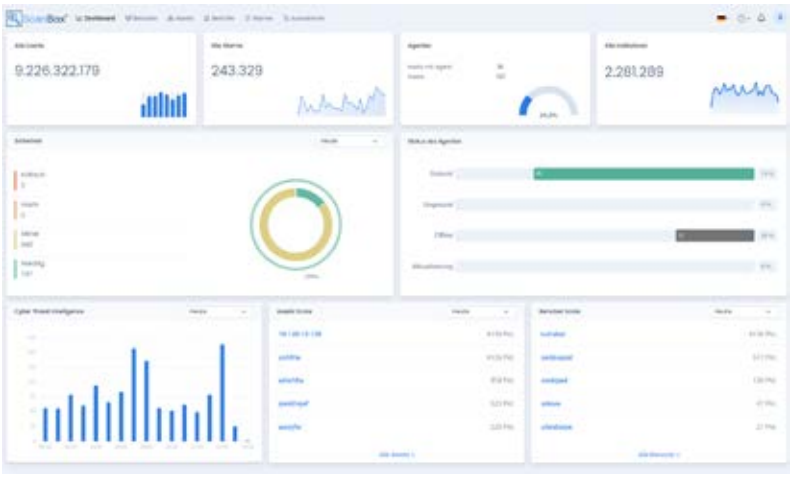
Die NIS-2-Richtlinie stellt eine umfassende Erweiterung der bisherigen Cybersicherheitsvorgaben dar. Die Umsetzung der Richtlinie verläuft vielerorts schleppend, auch in Unternehmen der kritischen Infrastruktur. Gründe sind unter anderem der hohe Zeitaufwand, die komplexen Anforderungen und der Fachkräftemangel. Vor diesem Hintergrund setzen viele Unternehmen auf technische Lösungen, die sie bei der Einhaltung der Vorgaben unterstützen.

Eine Möglichkeit zur Umsetzung der NIS-2-Anforderungen sind automatisierte Systeme zur Angriffserkennung und Netzwerküberwachung. Die ScanBox von DECOIT ist ein Beispiel für ein solches Werkzeug. Sie analysiert Netzwerkverkehr und Systemprotokolle, um Sicherheitsvorfälle frühzeitig zu erkennen.

„Die ScanBox wurde als unkompliziertes, skalierbares System zur Angriffserkennung entwickelt und nutzt als Basis aktuelle Bedrohungsdaten, um verdächtige Muster und Anomalien frühzeitig zu identifizieren“, zeigt Geschäftsführer Prof. Dr. Kai-Oliver Detken auf. Eine proaktive Verteidigung durch die schnelle Bedrohungserkennung und geeignete Gegenmaßnahmen werden ermöglicht. Durch die Anomalie-Erkennung werden Compliance-Abweichungen identifiziert und die Anzahl an „False Positives“ erheblich reduziert. Die zentrale Benutzeroberfläche der ScanBox (www.scanbox-product.de) ermöglicht proaktives Handeln ohne tiefergehendes Sicherheits- oder Clustermanagementwissen. Die Kombination aus benutzerfreundlicher Web-App und direktem Zugang zu Security-Analysten stellt ein Alleinstellungsmerkmal dar und ermöglicht eine erhebliche Zeit- und Personalentlastung.

Die ScanBox braucht nicht permanent an einen Mirror-Port angeschlossen werden, da die Switches zu sehr belastet werden und wertvolle Analysedaten verloren gehen können. Dafür wird bei der Netzwerkanalyse auf das Protokoll NetFlow gesetzt. Bei der Logfile-Analyse werden entsprechende Agenten auf den Client- und Serversystemen ausgerollt, die zusätzlich einen Anti-Viren-Schutz mitbringen. Die Kombination verschiedener Datenquellen verschafft ein Gesamtbild der Bedrohungslage. Ein Experten-Team steht immer direkt und persönlich zur Verfügung.

Die Umsetzung der NIS-2-Richtlinie stellt Unternehmen vor organisatorische und technische Herausforderungen. Analysewerkzeuge wie die ScanBox können eine Möglichkeit darstellen, die Einhaltung der gesetzlichen Vorgaben zu erleichtern und gleichzeitig Sicherheitsrisiken zu minimieren. Die ScanBox ist gerade für solche Unternehmen attraktiv, die keine High-End-Lösungen benötigen, aber die gesetzlichen Anforderungen der NIS-2-Richtlinie erfüllen müssen. ■



Das Dashboard zeichnet sich durch Benutzerfreundlichkeit und Übersichtlichkeit aus. Per Alarmfunktion wird der IT-Administrator unverzüglich über Anomalien unterrichtet. (Bild: DECOIT GmbH & Co. KG)

IT-Sicherheit ist Vertrauenssache

Machen Sie Ihr Unternehmen NIS2-Ready mit ESET Technologien aus der Europäischen Union

ESET® Digital Security
Progress. Protected.

eset.de/nis2

Sanktionen nach NIS-2

Bußgelder und Prozessorientierung im neuen IT-Sicherheitsrecht

„Wer nicht hören will, muss fühlen" gilt auch bei Regularien für Unternehmen. Allerdings sind Bußgelder bei Verstößen bei Weitem kein Automatismus – vielmehr gilt es, die genaueren Umstände zu beachten. Unsere Autoren erklären, wo man besonders aufpassen muss, aber auch, wann und weswegen eine Angst vor Sanktionen unbegründet ist.

Von Dennis-Kenji Kipker, Frankfurt/Main, und Julian Zaudig, Köln

Die effektive Durchsetzung des neuen BSI-Gesetzes (BSIG) gleicht der sprichwörtlichen Kunst des Möglichen: Es gilt, anspruchsvolle Sicherheitsstandards flächendeckend umzusetzen, ohne Unmögliches zu fordern oder den Innovationsgeist von Unternehmen zu ersticken.

Das BSIG verpflichtet Unternehmen zu erheblichen Investitionen in ihre IT-Sicherheit, oft jenseits des unmittelbaren betriebswirtschaftlichen Nutzens. Der Aufwand für die gesetzlich erforderlichen Sicherheitsmaßnahmen muss jetzt und in Zukunft nicht betriebswirtschaftlich durch einen „Sicherheitsgewinn" amortisiert werden. Vielmehr ist das Gemeinwohl entscheidend: Der Aufwand ist immer dann gerechtfertigt und verpflichtend, wenn er im angemessenen Verhältnis zu den wirtschaftlichen und gesellschaftlichen Folgen eines Ausfalls steht.

Unternehmen profitieren zwar im Ergebnis, wenn das Sicherheitsniveau in der deutschen Wirtschaft steigt, denn dies fördert eine sichere und resiliente Digitalisierung – erforderlich ist hierfür aber, dass das Sicherheitsniveau flächendeckend steigt. Diese Anforderung wirft die Frage auf, wie Maßnahmen durchgesetzt werden können, die sich für einzelne Betriebe – allen voran die vorbildlichen „First Mover" – möglicherweise nicht sofort rechnen.

An dieser Stelle offenbart sich die oft übersehene Doppelrolle von Bußgeldern im Wirtschaftsrecht: Sie fungieren nicht nur als Sanktionsinstrument, sondern auch als Garant der Wettbewerbsgerechtigkeit, weil sie ermöglichen, bei unrechtmäßig handelnden Unternehmen und Personen unrechtmäßige Vorteile abzuschöpfen (§ 17 Abs. 4 OWiG). Im IT-Sicherheitsrecht betrifft dies besonders Fälle, in denen Unternehmen das BSIG nicht oder nur unzureichend umsetzen, und dadurch gegenüber ihren rechtmäßig handelnden Mitbewerbern Kosten sparen. Bußgelder sollen die vermeintlichen Einsparungen in dem Fall nicht nur wettmachen (sog. Abschöpfungsteil), sondern sogar übersteigen (sog. Ahndungsteil).

Bußgelder für fairen Wettbewerb?

Die Europäische Kommission hatte bei Erarbeitung der NIS-2-Richtlinie eine klare Vorstellung und rügte ausdrücklich die mangelhafte Vollstreckung der IT-Sicherheitspflichten aus der NIS-1-Richtlinie in den Mitgliedstaaten: Insbesondere seien zu wenig Bußgelder verhängt worden – die NIS-2-Richtlinie solle dies ändern (siehe Ex-post-Bewertung in [1]).

IT-Sicherheitspflichten sollen zwar nach Art. 31 Abs. 2 der NIS-2-Richtlinie [2] risikobasiert beaufsichtigt und staatlich durchgesetzt werden können, um Aufsichtsbehörden die Fokussierung von Ressourcen zu ermöglichen. Allerdings war zentral, auch ein einheitliches und wirksames Aufsichtsniveau zu schaffen: Unternehmen sollen sich also im positiven wie im negativen Sinne darauf verlassen können, dass IT-Sicherheitspflichten durchgesetzt werden. Gerade Letzteres wird häufig übersehen, denn die gleichmäßige Durchsetzung von IT-Sicherheitspflichten war für die Europäische Kommission von vornherein auch eine Frage der Wettbewerbsgerechtigkeit (siehe Folgenabschätzung in [1]).

Aus Sicht eines CISO leuchtet das sofort ein: Ein Informationssicherheits-Managementsystem (ISMS) entsprechend dem BSIG, nimmt nicht nur den eigenen Betrieb in den Blick, sondern auch das Gemeinwohl. Wie soll man diese Aufwendungen gegenüber den eigenen Stakeholdern rechtfertigen, wenn direkte Konkurrenten die gesetzlichen Vorgaben ohne Konsequenzen ignorieren? Erschwert die IT-Sicherheitsabteilung dem eigenen Unternehmen dann nicht sogar, sich im Wettbewerb zu behaupten? Die Kommission trifft einen praktischen Punkt: Ein Gesetz, das flächendeckend verpflichtet, aber nur die Willigen zwingt, leidet an einem grundlegenden Mangel – es ist nicht nur unzweckmäßig, sondern auch noch ungerecht.

Das BSI will bei der nationalen Umsetzung durch das NIS-2-Umsetzungs- und Cybersicherheitsstärkungs-Gesetz (NIS2UmsuCG, vgl. [4]) dennoch auf Kooperation setzen – und dieser Ansatz ist nachvollziehbar wie gleichermaßen positiv. Denn tatsächlich ist der Wert von Kooperation im Rahmen der Aufsicht über die gesetzlichen Cybersicherheitspflichten kaum zu überschätzen, weil das BSIG systematisch auf Kooperation zwischen Aufsichtsbehörde und Unternehmen baut: Das BSI steht in der Mitte des Informationsflusses zwischen den wesentlichen und wichtigen Einrichtungen – es ist und bleibt die zentrale Plattform über den Austausch zu Cybersicherheit und Bedrohungen für ebenjene. Ferner ist es eben nicht bloß Aufgabe des BSI, Unternehmen zu beaufsichtigen, sondern ebenso diese zu beraten.

Vom Gesetzestext zur Praxis

Eine systematische rechtliche Analyse zeigt auch, dass der Konflikt zwischen Beratung und Aufsicht durch und mithilfe von Bußgeldern in der Praxis entschärft sein wird – und zwar mit bewährten Mitteln. Jeder Jurist lernt in seiner Ausbildung sehr früh: Strafrecht – und dazu zählen letztlich auch Bußgelder – ist „ultima ratio", also stets das letzte Mittel. Bußgelder anders anzuwenden, wäre nicht sinnvoll und in vielen Fällen schlicht rechtswidrig.

Die erste Frage, die sich in diesem Zusammenhang stellt, ist die offensichtliche: Darf das BSI von Bußgeldverfahren absehen? Die klare Antwort lautet: ja. In Deutschland muss nicht jede Ordnungswidrigkeit verfolgt werden. Die Behörden haben hier schon allgemein ein sogenanntes „Aufgreifermessen", das ihnen erlaubt, Schwerpunkte zu setzen und risikobasiert zu arbeiten. Willkür ist dabei verboten – eine sachlich-pragmatische Entscheidungsfindung steht Behörden aber stets offen. Das BSI darf auch Leitlinien für seine Bußgeldentscheidungen kommunizieren.

Die Grenze findet dieses Aufgreifermessen aber in dem Gesetzesvollzug an sich. Deshalb ist wichtig, dass das BSI erklärt, vorrangig auf Kooperation zu setzen, nicht aber ausschließlich – dies wäre wiederum rechtswidrig. Denn das Aufgreifermessen verbietet einer Behörde, ein Gesetz schlicht unberücksichtigt zu lassen. In anderen Worten: Entscheidet der Gesetzgeber, dass Bußgelder verhängt werden sollen, darf die Behörde entscheiden, in welchen Fällen dies sinnvoll ist. Sie darf sich jedoch nicht zum Gesetzgeber aufschwingen und von Bußgeldern generell absehen.

Die Leitlinie bei Bußgeldentscheidungen wurde vielmehr vom Europäischen Gesetzgeber fixiert und folgt aus Art. 34 Abs. 1 der NIS-2-Richtlinie: Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein. Diese Maßgabe muss auch das BSI beachten (sog. unionsrechtskonforme Auslegung).

Inhaltliche Reichweite der Tatbestände

Für Verantwortungsträger ist dies allerdings nicht endgültig zufriedenstellend: Denn hiernach hat das BSI grundsätzlich Bußgelder in Erwägung zu ziehen; in begründeten Fällen *kann* es bloß auf sie verzichten. Sogar wenn ein Unternehmen sich um Selbstkorrektur bemüht, bedeutet dies deshalb *nicht,* dass das BSI auch von einem Bußgeld absehen *muss.*

Daraus folgt die Anschlussfrage: Was ist konkret mit Bußgeld bedroht? Das BSIG enthält weitreichende Bußdrohungen, denn es setzt auf sogenannte „Blankettnormen". Diese zeichnen sich dadurch aus, dass sie keine eigenen Tatbestände enthalten, sondern auf andere Vorschriften verweisen. Zumindest dem Wortlaut nach ergibt sich deshalb ein automatisches Bußgeldrisiko: Wer eine Sicherheitsmaßnahme aktuell entgegen § 8a Abs. 1 BSIG oder künftig entgegen § 30 Abs. 1 BSIG nicht umsetzt, wird zwar nicht automatisch mit einem Bußgeld belegt, wohl aber gemäß § 14 Abs. 2 Nr. 2 BSIG und künftig gemäß § 65 Abs. 2 Nr. 2 BSIG mit Buße bedroht. Dieser weite Wortlaut erklärt auch, weswegen diese Vorschriften in der öffentlichen Wahrnehmung und bei der Geschäftsleitung von betroffenen Betrieben so hohe Wellen schlagen.

Auch rechtmäßige ISMS müssen nicht „perfekt" sein

Für den Sicherheitspraktiker ist diese unbeschränkte Bußdrohung irritierend, denn aus den Vorschriften des BSIG geht weder jetzt noch in Zukunft hervor, welche Sicherheitsmaßnahmen konkret zu ergreifen sind. Es gibt zwar einen Katalog von Mindestsicherheitsmaßnahmen (künftig: § 30 Abs. 2 BSIG) – aber auch wenn diese ergriffen werden, gewährleistet dies noch nicht die Compliance des eigenen ISMS. Hierfür müssen über die Mindestsicherheitsmaßnahmen hinaus auch die „angemessenen" Sicherheitsmaßnahmen nach § 30 Abs. 1 BSIG implementiert werden, welche im Übrigen dem Stand der Technik entsprechen „sollen".

Diese Rechtsbegriffe sind hochgradig abstrakt und weder technisch noch organisatorisch eindeutig umsetzbar. Stattdessen zeigt sich sprachlich Folgendes: Das BSIG zwingt Sicherheitsverantwortliche jetzt und in Zukunft zu einer Entscheidung; welche Sicherheitsmaßnahmen umgesetzt werden und welche nicht, zeichnet diese Entscheidung aber nicht konkret vor. In der juristischen Debatte wird dies als „juristisches Patt" bezeichnet, in dem keine der Handlungsalternativen *erkennbar* rechtmäßig ist [6].

Hier muss man sich ins Gedächtnis rufen, woraus diese gesetzliche Unschärfe methodisch folgt: Ein ISMS ist hochgradig individuell. Im Kern stehen Prognoseentscheidungen: Welches Risiko verwirklicht sich und welche Gegenmaßnahmen sind in einem konkreten Betrieb auch wirksam? Diese Prognoseentscheidungen stellen sich erst im Nachhinein als „richtig" oder „falsch" heraus. Im Moment ihrer Vornahmen sind sie aber nur sorgfältig begründet oder gerade unbegründet. Der Praktiker weiß: Mehr als sorgfältig arbeiten kann man nicht – und auch wenn man sorgfältig arbeitet, kann man keine absolute Sicherheit erreichen oder versprechen.

Technische Normen reagieren darauf mit einer iterativen Selbstüberprüfung und Selbstkorrektur. Nur zu diesem sorgfältigen Prozess, nicht aber zur „richtigen" Risikoentscheidung, einem „richtigen" ISMS oder gar zum „Zustand der IT-Sicherheit" kann das BSIG zwingen (vgl. EuGH-Urteil [7] sowie [8] und [6], S. 292 ff.). Juristen haben auch hierfür schon seit langem einen Begriff: „Ultra posse nemo obligatur" – zu Unmöglichem ist niemand verpflichtet.

Verfassungskonforme Unschärfe?

Sprechen bereits Juristen von einer Pattsituation, erscheint fragwürdig, ob eine solche Regelung überhaupt zulässig ist. Rechtlich stellt sich die Frage nach der „hinreichenden Bestimmtheit" einer Vorschrift: Diese ist auch für den Gesetzgeber nicht beliebig, vielmehr setzt die Verfassung der Unbestimmtheit von Gesetzen Grenzen. Die Prüfung dieser Grenzen stellt jedoch selbst eine Herausforderung dar, denn offensichtlich kann man die „Bestimmtheit" eines Gesetzes nicht quantitativ bemessen: Gesetze bestehen aus Sprache und Sprache kann per se nicht eindeutig sein. Die Rechtsprechung prüft die hinreichende Bestimmtheit einer Norm deshalb anhand einer Abwägung und beurteilt, ob bestehende Unklarheiten einer gesetzlichen Regelung – in Form einer Negativabgrenzung – noch hinnehmbar sind.

Aus dieser Abwägung ergibt sich im IT-Sicherheitsrecht eine ganz wesentliche Unterscheidung: Was im Allgemeinen gilt, muss nicht für die Bußnormen gelten. Denn auch ein Bußgeld stellt verfassungsrechtlich eine Strafe dar – und Strafvorschriften sind an strengeren Maßstäben zu messen als Rechtsvorschriften im Allgemeinen. Auch hierfür haben Juristen einen seit langem feststehenden Begriff: „Nulla poena, nullum crimen sine lege certa" – keine Strafe ohne *bestimmtes* Gesetz.

Auch dieser Grundsatz ist für den Praktiker ohne Weiteres verständlich: Selbstverständlich ist es häufig hilfreich, Regelungen nicht allzu detailliert zu fassen, sondern Umsetzungsspielräume zu belassen. Nur so bleiben auf der Arbeitsebene passende, auf den einzelnen Anwendungsfall abgestimmte Lösungen erlaubt. Gerade im technischen Bereich arbeitet man deshalb bewusst mit Frameworks statt starrer Pflichtenkataloge. Anders ist dies jedoch, wenn jemandem Fehlverhalten vorgeworfen werden soll: Ein Vorwurf muss konkret sein, sonst kann sich der Betroffene weder angemessen verteidigen, noch kann er sich verbessern – schon weil er sonst gar nicht konkret wüsste, was er falsch gemacht haben soll.

Dieser im Kern sehr praktischen Einsicht folgt auch die Rechtsprechung des Bundesverfassungsgerichts. Zwar ist grundsätzlich stets zu fordern, dass jedermann vorhersehen kann, was von ihm gefordert wird, um sich rechtmäßig zu verhalten. Auch wenn dies im Einzelfall nicht möglich ist, bleibt der Gesetzgeber allerdings befugt, dennoch Regelungen zu erlassen. Die Unbestimmtheit folgt dann aus der „Natur der Sache" – im IT-Sicherheitsrecht zum Beispiel aus der Dynamik der Bedrohungslage, die es verbietet, Sicherheitsmaßnahmen statisch zubeschreiben – und rechtfertigt eine Unbestimmtheit von Vorschriften, die etwa Sicherheitsmaßnahmen nach dem „Stand der Technik" fordern. Sicherheitsmaßnahmen mit dem „Stand der Wissenschaft und Technik" zu umschreiben, wurde deshalb auch hinsichtlich der Sicherung von Kernkraftwerken für zulässig gehalten (BVerfG-Urteil vom 8. August 1978, Az. 2 BvL 8/77 „Schneller Brüter").

Hinsichtlich der Bußgelder gelten jedoch andere Maßstäbe, denn hier gilt das spezielle strafrechtliche Bestimmtheitsgebot nach Art. 103 Abs. 2 des Grundgesetzes (GG – vgl. BVerfG-Urteil vom 11. Januar 1995, Az. 2 BvR 1473/89). Und dieses spezielle Bestimmtheitsgebot fokussiert auf den Schutz des Einzelnen: Jeder muss vorhersehen können, was mit Strafe bedroht ist. Erlaubt sind allenfalls „Randunschärfen" (vgl. BVerfG-Urteil vom 23. Juni 2010, Az. 2 BvR 2559/08).

Diese strafrechtliche Bestimmtheit lässt sich nach der Rechtsprechung des Bundesverfassungsgerichts (BVerfG) auf zwei Arten herstellen: Entweder die Sanktionsvorschrift kann selbst konkret darstellen, was mit Bußgeld bedroht ist, oder die zu dieser Vorschrift ergangene Rechtsprechung muss dies erkennen lassen (BVerfG-Urteile vom 28. Juni 2015, Az. 2 BvR 2558/14, 2 BvR 2571/14 und 2 BvR 2573/14). Diese Konkretisierung von Rechtsvorschriften soll im Bereich des Straf- und Bußgeldrechts sogar Aufgabe der Rechtsprechung sein (BVerfG a. a. O.). Fehlt eine solche Konkretisierung (noch), erlaubt das Grundgesetz aber keine für den Bürger unvorhersehbare Strafe – und damit auch kein entsprechendes Bußgeld.

Deshalb gilt aktuell noch für § 14 Abs. 2 Nr. 2 BSIG beziehungsweise künftig für § 65 Abs. 2 Nr. 2 BSIG: Der Tatbestand dieser Sanktionsvorschriften reicht nicht so weit, wie er sich liest. Niemand darf „raten" müssen, wann er mit einem Bußgeld belegt werden kann – von

einem Zweifelsrisiko ist er zu befreien. Deshalb ergibt sich jetzt und in Zukunft: Mit Buße bedroht sind nur offen erkennbar unzureichende Sicherheitsmaßnahmen [6].

Jeder Verantwortliche ist jedoch gut beraten, die Rechtsprechung im IT-Sicherheitsrecht engmaschig zu beobachten, weil sich hieraus in Zukunft jederzeit Änderungen ergeben können. Dies ist ein weiterer Umstand, der zeigt: Der CISO füllt aufgrund des BSIG nicht länger eine rein technische, sondern eine interdisziplinäre Rolle aus, die Technik, Recht und Wirtschaftlichkeit vereinen muss.

Konkretisierung von Bußgeld-Risiken

Aufbauend auf diesen Erkenntnissen lassen sich verschiedene Fallgruppen zum rechtskonformen IT-Sicherheitsmanagement nach NIS-2 ableiten:

_____ *„Das betrifft uns nicht":* Wer nicht erkennt, dass er vom BSIG erfasst ist, kann mit einem Bußgeld belegt werden. Hier besteht keine unüberwindbare rechtliche Unsicherheit, denn mit Inkrafttreten des NIS2UmsuCG lässt sich die Betroffenheit des eigenen Unternehmens rechtssicher feststellen.

_____ *„Abkürzungen" und „Sparen" im Rahmen des übrigen ISMS:* Wessen reguliertes ISMS an grundlegenden Mängeln leidet, kann (und sollte!) mit einem Bußgeld belegt werden. Zur Illustration kann auf die Beispiele zur Organhaftung in der vorigen <kes> [8] zurückgegriffen werden. Es gilt: Wer fahrlässig oder sogar vorsätzlich „Abkürzungen" nimmt und sich dadurch einen illegalen Vorteil verschafft, dem kann und sollte dieser Vorteil durch ein Bußgeld genommen werden.

_____ *Weithin unbeachtete betriebliche Sicherheitsrichtlinie(n):* Man kann gar nicht oft genug betonen, dass ein ISMS zwar naturgemäß auf betrieblichen Richtlinien, Anweisungen und Dokumentationen aufbaut, im Rahmen des BSIG dann allerdings nicht die Papierlage, sondern die tatsächliche Umsetzung von Sicherheitsmaßnahmen überprüft wird (vgl. [7,8]). Wer hier spart, dem droht ebenso ein Bußgeld.

_____ *Nicht „Stand der Technik":* Ein Bußgeld kann nicht verhängt werden, weil von technischen Richtlinien – gerade des BSI – abgewichen wird. Die Äußerungen des BSI gegenüber Unternehmen sind hier teilweise missverständlich: Der Stand der Technik muss eben nicht „langsam aber sicher" erreicht werden – richtig ist: Der Stand der Technik soll *unmittelbar nach Geltung* des NIS2UmsuCG eingehalten werden (künftig § 30 Abs. 2 Satz 1 BSIG), muss aber jetzt und in Zukunft *nicht flächendeckend* erreicht werden. Eine gut begründete Entscheidung gegen technische Standards ist deshalb rechtmäßig und zieht kein Bußgeld nach sich.

_____ *Schlichte Fehleinschätzungen und Implementierungsfehler:* Auch einzelne Fehler, wie ein Augenblicksversagen auf der Arbeitsebene, nimmt das Gesetz zuletzt hin, insoweit im Übrigen sorgfältig gearbeitet und korrekt reagiert wird. Absolute Sicherheit ist unerreichbar, also darf auch kein Bußgeld ergehen, nur weil jemand sie nicht erreicht.

In der Gesamtschau zeigt sich folglich: Ein Automatismus dahingehend, dass jeder Verstoß gegen IT-Sicherheitspflichten ein Bußgeld begründet, besteht – unabhängig von der Praxis des BSI – schon kraft Gesetzes gerade nicht. Hiervor müssen sich also weder CISOs noch sonstige Verantwortungsträger sorgen.

Wer aber denkt, er könne im regulierten Bereich „sparen" oder „Abkürzungen" nehmen, der bewegt sich auf dünnem Eis: Dies sind Fälle, in welchen Bußgelder sehr naheliegen!

Vertrauen ist gut, Compliance ist besser

Im Rahmen der Bußgelder ist die Haltung des BSI vor diesem gerade skizzierten rechtlichen Hintergrund eine gute Nachricht. Sie sollte jedoch auch nicht täuschen: Es wird keine rein kooperative Aufsicht geben. Dies wäre erstens rechtswidrig und würde die Bundesrepublik zweitens wahrscheinlich in einen Konflikt mit der Europäischen Kommission führen, welche Bußgelder als zentral zur Durchsetzung der Regelungen von NIS-2 ansieht.

Man darf zudem nicht vergessen, an wen sich das BSI mit seinen öffentlichen Aussagen wendet: an diejenigen, die sich informieren und IT-Sicherheit richtig und rechtmäßig umsetzen wollen – andere jedoch, die denken oder sogar darauf spekulieren, NIS-2 werde zukünftig nicht vollzogen, sind damit nicht gemeint. Schon die Kommission hat richtig erkannt: In diesen Fällen Bußgelder zu verhängen, ist nicht nur rechtmäßig, sondern auch eine Frage der Fairness gegenüber allen anderen.

Für CISOs ergeben sich daraus zwei wesentliche Schlussfolgerungen:

_____ *Sorgfältige Prozessarbeit ist ein Schutzschild gegen Bußgelder:* Wer sich ehrlich um Compliance bemüht, muss keine Sorge vor Bußgeldern haben. Denn auch ein reguliertes ISMS nimmt einzelne Fehler hin und verlangt keine Perfektion – gerade das ist ja der betriebsorganisatorische Ansatz eines ISMS. Das Vorgehen des BSI zeigt: Es will keine Bußgelder verhängen müssen – dabei ist es aber an Recht und Gesetz gebunden. Dem BSI müssen betroffene Unternehmen also Argumente liefern, weswegen ein Bußgeld eben nicht erforderlich oder sogar unverhältnismäßig ist. Deshalb ist eine betriebliche IT-Sicherheits-Dokumentation auch von so entscheidender Bedeutung.

Im Verhältnis zur Aufsichtsbehörde kann für die Arbeit der IT-Sicherheitsabteilung deshalb als klare Zielsetzung definiert werden, dass sie in der Lage sein muss, *jederzeit darzulegen, dass und wie man sich auch ohne Einschreiten des BSI an Recht und Gesetz hält.* Hierfür ist die rechtliche Ebene in die technischen Standards zu integrieren: Sicherheitsmaßnahmen sind nicht nur sorgfältig auszuwählen und zu dokumentieren, vielmehr muss man auch festhalten, weswegen man sie für rechtmäßig hält. Das wird leider zu häufig übersehen. Und diese Prägung erfasst auch den PDCA-Kreislauf: Maßnahmen sind nicht nur daraufhin zu überprüfen, ob sie wirksam sind – zusätzlich ist darauf zu achten, ob ihre rechtliche Begründung (weiterhin) trägt und ein rechtmäßiger Betrieb sichergestellt ist.

CISOs, die diese interdisziplinäre Arbeit meistern, werden sich der Aufsichtsbehörde als integrer und vertrauenswürdiger Partner präsentieren können. In Krisensituationen kann das Gold wert sein – nach § 65 Abs. 5 Nr. 1 Lit. a BSIG bis zu 10.000.000 €.

All das bedeutet im Ergebnis: Man kann gegenüber betroffenen Stakeholdern durchaus auch mit drohenden Bußgeldern argumentieren, damit die Wirksamkeit des NIS2UmsuCG nicht infrage gestellt wird. Aber dann sollte man richtiger- und fairerweise auch betonen: Sicherheitslücken ziehen nicht automatisch Bußgelder nach sich. Bußgelder sind nicht der „Preis" für Sicherheitslücken oder Abweichungen vom Stand der Technik – sie sind vielmehr der Preis dafür, wenn das NIS2UmsuCG insgesamt nicht ernst genommen wird. ■

Prof. Dr. Dennis-Kenji Kipker ist wissenschaftlicher Direktor des cyberintelligence.institute in Frankfurt am Main.

Dr. Julian Zaudig ist Volljurist und wurde von der Universität zu Köln zum IT-Sicherheitsrecht promoviert. Er forscht an der Schnittstelle von Recht und Technik – neben seiner juristischen Ausbildung in Stellen wie der Zentral- und Ansprechstelle Cybercrime NRW sowie der Stiftung Familienunternehmen und Politik war er auch technisch und unternehmerisch tätig.

Literatur

[1] Europäische Kommission, Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148, Dezember 2020, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52020PC0823

[2] Europäische Union, Richtlinie (EU) 2022/2555 Des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie), in: Amtsblatt der Europäischen Union L 333, S. 80, Dezember 2022, berichtigt im Dezember 2023, konsolidierte Fassung: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:02022L2555-20221227

[3] Dario Scholz, Dennis-Kenji Kipker, EU-Cybersecurity Version 2.0, Bringt NIS-2 das lang ersehnte Update für wesentliche und wichtige Einrichtungen?, <kes> 2023#1, S. 19

[4] Dennis-Kenji Kipker, NIS2UmsuCG: Das NIS-2-Umsetzungs- und Cybersicherheitsstärkungs-Gesetz kommt – ein Überblick über den Status quo, <kes> 2023#4, S. 70

[5] Denis-Kenji Kipker, Auf der Suche nach dem Heiligen Gral der Cybersicherheit?, <kes>2024#3, S. 13

[6] Julian Zaudig, Die Regulierung von Risiken durch den Einsatz von Informationstechnik nach dem BSIG, Der rechtmäßige Umgang mit ungewissen Entwicklungen durch Unternehmen und Geschäftsleiter im Bereich der IT-Sicherheit, Nomos, August 2024, ISBN 978-3-7560-1612-9

[7] Europäische Union, Urteil des Gerichtshofs (Dritte Kammer) vom 14. Dezember 2023, VB gegen Natsionalna agentsia za prihodite, Rechtssache C-340/21, Dezember 2023, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:62021CJ0340

[8] Dennis-Kenji Kipker, Julian Zaudig, Schutzschild gegen Haftungsrisiken, Wie die Rolle des CISO unter NIS-2 neu gedacht werden muss, <kes> 2024#5, S. 32

[9] Bundesministerium des Innern und für Heimat (BMI), Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz), Gesetzentwurf der Bundesregierung, Juli 2024, www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/kabinettsfassung/CI1/nis2-regierungsentwurf.pdf?__blob=publicationFile