LOGPOINT

Auf der Überholspur: NIS-2 im Unternehmen schnell umsetzen

www.logpoint.com

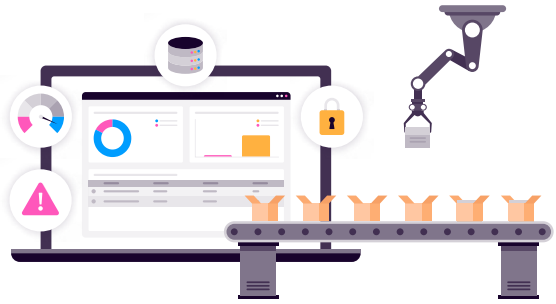
Auf der Datenautobahn lauern Gefahren: Unternehmen – nicht zuletzt die Betreiber kritischer Infrastruktur (KRITIS) – waren noch nie so großen Cyberrisiken ausgesetzt wie heute. Deshalb ist Deutschland gefordert, bis 2024 die verschärfte NIS-2-Direktive der EU zur Cybersicherheit umzusetzen.

Rund 40.000 deutsche Unternehmen gelten als wichtig oder sehr wichtig für die Volkswirtschaft und sind somit von den strengeren Vorgaben betroffen – und bei Verstößen drohen Strafen bis in Millionenhöhe. Dieses Whitepaper erläutert die Anforderungen von NIS 2 und zeigt auf, wie Unternehmen sie möglichst einfach erfüllen können.

GURTPFLICHT FÜR DIE IT

„Bei einem Unfall stütze ich mich einfach am Lenkrad ab!“ Solche Aussagen von Autofahrern waren in den 1970er-Jahren in Deutschland oft zu hören. Denn die Gurtpflicht, am 1.1.1976 in Kraft getreten, sorgte für lebhafte Diskussionen und einigen Widerstand. Heute hingegen möchte bei einem Autounfall niemand mehr Gurt und Airbags missen. Ganz anders im Geschäftsleben: Inzwischen sind praktisch alle Unternehmen von reibungslos funktionierender IT abhängig, aber allzu viele Verantwortliche unterschätzen, wie einst die Autofahrer, das Risiko. Sie verlassen sich leichtsinnigerweise darauf, den Aufprall eines Cyberangriffs mit altbewährter „Muskelkraft“ abfedern zu können. Dem schiebt nun eine neue EU-Richtlinie einen Riegel vor.

Schon 2016 führte die EU eine „Anschnallpflicht“ für kritische Infrastrukturen und deren digitalen Unterbau ein: In der NIS-Richtlinie (Network and Information Security Directive EU 2016/1148) legte sie EU-weite Regeln für deren Cybersicherheit fest. Doch viele Betreiber kritischer Infrastrukturen setzten diese Vorgaben nur halbherzig um und meldeten Vorfälle nicht. Deshalb verschärfte die EU in der NIS-2-Richtlinie (NIS 2 Directive EU 2022/2555), gültig seit Anfang 2023, ihre Anforderungen an die KRITIS-Betreiber und dehnte sie zugleich auf weitere Unternehmen aus, die für die Versorgung der europäischen Volkswirtschaften relevant sind.



Denn veraltete oder laxe IT-Sicherheitskonzepte öffnen Tür und Tor für Cybergefahren wie zum Beispiel Ransomware (Erpressersoftware, die Daten zwangsverschlüsselt und nur gegen Lösegeld wieder freigibt), ebenso für Industriespionage oder Sabotage. Das zeigen die aktuellen Zahlen des IT-Branchenverbands Bitkom: Demnach entsteht der deutschen Wirtschaft durch Diebstahl von Daten oder IT-Equipment, Spionage und Sabotage ein jährlicher Schaden von rund 206 Milliarden Euro. Knapp drei Viertel (74 Prozent) der Unternehmen waren im letzten Jahr von solchen Angriffen betroffen, weitere acht Prozent vermuten dies. Cyberangriffe haben auch eine weltpolitische Dimension: 46 Prozent der betroffenen Unternehmen haben mindestens einen Angriff aus Russland festgestellt, 42 Prozent einen aus China.

Vor diesem Hintergrund sind nun die EU-Länder in der Pflicht, die NIS-2-Richtlinie bis Oktober 2024 in Gesetze zu gießen. In Deutschland ist dazu das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) in Arbeit, das seit Juli 2023 als **zweiter Referentenentwurf** vorliegt.

ERHÖHTER HANDLUNGSBEDARF

Die kommende NIS-2-Gesetzgebung erhöht für Geschäftsführer und weitere Verantwortliche in zahlreichen Unternehmen aus dreierlei Gründen den Druck: Erstens dehnt NIS 2 den Geltungsbereich auf alle Unternehmen mit +100 Mitarbeitern oder +10 Millionen Umsatz weitere Branchen aus. Zweitens führt NIS 2 für geschäftsrelevante Vorfälle eine Berichterstattungspflicht ein. Und drittens drohen bei Verstoß gegen NIS-2-Vorgaben nun Strafzahlungen in Höhe von bis zu zehn Millionen Euro oder zwei Prozent des Jahresumsatzes eines Unternehmens. Im Rahmen der Debatte um den NIS2UmsuCG-Entwurf ist sogar eine persönliche Haftung des Geschäftsführers im Gespräch, falls dessen mangelhaftes Risikomanagement dazu führt, dass sein Unternehmen NIS-2-Anforderungen nicht angemessen umsetzt.

Zugleich wächst die Liste der Unternehmen, die unter das Gesetz fallen, erheblich. Denn die EU-Länder sollen gegenüber Cyberangriffen resilienter werden, indem mehr Branchen ihre Cybersicherheit verstärken. Statt den knapp 5.000 KRITIS-Betreibern der bisherigen NIS-Gesetzgebung gelten nun zirka 40.000 Unternehmen und Organisationen in Deutschland als schutzrelevant, NIS kannte nur sieben KRITIS-Branchen; NIS 2 hingegen umfasst 18 Branchen und Sektoren, unterteilt in elf „besonders wichtige“ Bereiche („Essential Entities“) und sieben „wichtige“ Bereiche („Important Entities“). Eine Checkliste, an der Unternehmen herausfinden können, ob sie betroffen sind, findet sich hier.

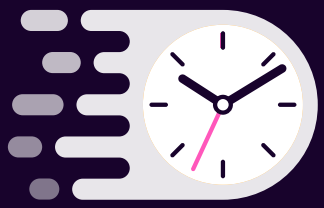
Zu den „besonders wichtigen“ Bereichen zählen die Energieversorgung, der Transport, das Gesundheitswesen, Banken, Finanzmärkte, die öffentliche Verwaltung, die Raumfahrt, die Wasserversorgung (Trink- wie auch Abwasser), digitale Infrastrukturen (also zum Beispiel Internetknoten, Cloud-Provider und RZ-Betreiber) sowie das ITK-Management im B2B-Bereich (beispielsweise Managed Service Provider). Die Schwellenwerte für die Unternehmen in diesen Sektoren liegen bei 250 Mitarbeitern und einem Umsatz von 50 Millionen Euro oder einer Bilanzsumme von 43 Millionen Euro. Unabhängig von der Größe können Unternehmen aber als besonders wichtige Organisationen eingestuft werden.

Die neu eingeführten „wichtigen“ Segmente umfassen Postdienste, die Abfallwirtschaft, die Chemieindustrie, Forschungsinstitute, die Lebensmittelbranche (Herstellung und Vertrieb), bestimmte Industriebereiche (Fahrzeugbau, Maschinenbau, medizinischer Geräte etc.) sowie Anbieter von digitalen Diensten wie Marktplätzen, sozialen Netzwerken oder Suchmaschinen. Die Erfassungsschwelle liegt hier deutlich niedriger: bei 50 Mitarbeitern und einer Umsatz- oder Bilanzsumme von zehn Millionen Euro. Deshalb sind hierzulande nun allein in diesen Branchen über 20.000 Unternehmen bald verpflichtet, nachweislich Mindeststandards der Cybersecurity einzuhalten.

DIE VERSCHÄRFTEN VERKEHRSREGELN IM ÜBERBLICK

NIS 2 stellt einige Cybersecurity-„Verkehrsregeln“ auf. Diese betreffen vier Bereiche: das Risikomanagement, die Verantwortlichkeiten im Unternehmen, das Reporting bei Vorfällen sowie die Gewährleistung des unterbrechungsfreien Geschäftsbetriebs („Business Continuity“). Im Fall eines Cyberangriffs ist eine schnelle Reaktion inklusive Störungsmeldung vorgeschrieben. Eine erste Meldung (à la „Houston, wir haben ein Problem“) ist dem Bundesamt für Sicherheit in der Informationstechnik (BSI) innerhalb von 24 Stunden nach Entdeckung eines geschäftsrelevanten Vorfalls zu übermitteln, eine detaillierte Vorfallsmeldung muss binnen 72 Stunden erfolgen.

Eine derart zügige Reaktion erfordert die automatisierte Überwachung der IT-Infrastruktur mit ebenso automatisierter Alarmierung bei Verdachtsfällen. Dazu ist eine Reihe von technischen und organisatorischen Maßnahmen zu ergreifen. Das Unternehmen muss nachweislich einen IT-Security-Prozess inklusive eines Eskalationsteams einrichten und dabei den „Stand der Technik“ umsetzen. Dieser „Stand der Technik“ ist sinnvollerweise nicht im Detail spezifiziert, da er sich in der IT-Welt sehr schnell weiterentwickelt. Laut BSI umfasst dieser Stand der Technik vorrangig ein ISMS (Information Security Management System), also ein System zur Überwachung der Informationssicherheit, wie es auch die **ISO 27001:22** vorschreibt.



Der Kernbaustein eines solchen ISMS Systems ist eine sogenannte SIEM-Lösung (Security Information and Event Management). Eine SIEM-Lösung sammelt über die gesamte IT-Infrastruktur hinweg Meldungen der Überwachungswerkzeuge und -sensoren, bündelt diese zu Alarmen und gibt diese dann auf den vorgegebenen Kanälen aus. Sie gleicht damit der Alarmanlage eines modernen Autos.

Ergänzend empfehlen Fachleute eine Lösung, die auch das Verhalten der IT Nutzer und Administratoren und deren Endgeräte laufend überwacht (UEBA genannt). Denn zahlreiche Angriffe erfolgen heutzutage durch Insider, etwa durch Beschäftigte, die sich über eine Abmahnung oder gar Kündigung ärgern. Die Rache soll dann den Arbeitgeber treffen oder aber es wird sogar Lösegeld gefordert, dazu muss die Nutzung und Anwendung DSGVO-relevanter Daten besonders gegenüber Missbrauchsversuchen geschützt werden.

Zu den technischen Anforderungen gesellen sich organisatorische: Das Unternehmen muss zum Beispiel Risikobewertungen erstellen und Sicherheitsrichtlinien einführen, ebenso Verfahren, um die Wirksamkeit seiner Sicherheitsmaßnahmen zu evaluieren. Es muss Notfallpläne für die Geschäftskontinuität erarbeiten und eine Überwachung seiner Lieferketten einrichten. Nicht zuletzt muss das Unternehmen seine Belegschaft mit Cybersicherheits-Schulungen für Angriffe sensibilisieren.

SPURHALTE-ASSISTENT ZU KLAR KALKULIERBAREN KOSTEN

Die geforderten organisatorischen Maßnahmen sind bei jedem Unternehmen, das unter NIS 2 fällt, individuell. Jede Organisation muss sie für sich selbst erarbeiten und umsetzen. Einfacher sieht es zum Glück bei den technischen Maßnahmen aus, insbesondere bei der laufenden Überwachung der IT-Infrastruktur durch ein SIEM-System. Hier hat ein Unternehmen drei Möglichkeiten.

1. Erstens kann es in gewohnter Weise Hardware beschaffen, eine SIEM-Software installieren und sein IT-Team mit der Bedienung, Wartung und dem Handling der Alarme betrauen. Dazu wird es oft erforderlich sein, einen oder mehrere Security-Spezialisten zusätzlich einzustellen – in Zeiten akuten IT-Security-Fachkräftemangels kein leichtes Unterfangen. Die neuen NIS-2-Vorgaben werden diesen Fachkräftemangel wohl noch weiter verschärfen, stehen doch nun Tausende Unternehmen vor den gleichen verschärften Security-Herausforderungen.

2. Eine Alternative zum lokalen SIEM-Betrieb ist der Bezug der Software aus der Cloud. Dies erübrigt die Beschaffung und Wartung lokaler Hardware, löst aber nicht das Personalproblem beim SIEM-Einsatz.

3. Der dritte und am leichtesten gangbare Weg ist deshalb der Bezug von SIEM als Managed Service. Hier übernimmt der Managed Service Provider den Betrieb der Lösung in der – natürlich NIS-2-konformen – Cloud und sorgt für die laufende Überwachung definierter Sicherheitsprozesse als Security Operation Center (SOC). Das Anwenderunternehmen muss dann lediglich mit seinem hausinternen IT-Team dafür sorgen, dass Alarme im Fall einer Betriebsstörung behoben werden und an die zuständigen Stellen gemeldet werden.

SIEM als Managed Service macht die Kosten für die Absicherung der IT-Arbeitsplätze gemäß NIS 2 so einfach kalkulierbar wie Leasing-Aufwendungen für einen Dienstwagen. Ein Rechenbeispiel: Die Kosten durch einen Ransomware-Angriff belaufen sich laut Medienberichten im Schnitt auf 1,6 Millionen Euro pro Vorfall – die Lösegeldzahlung selbst noch gar nicht mitgerechnet. Dem gegenüber stehen bei Managed SIEM überschaubare Fixkosten zu Preisen ab 40 Euro pro IT Arbeitsplatz und Jahr. Ein „wichtiges“ Unternehmen mit 100 Computer-Arbeitsplätzen kann sich also mit geringem finanziellem Aufwand pro Jahr vor unkalkulierbar teuren Cybervorfällen schützen zugleich einen Kernbaustein seiner NIS-2-Konformität nachweisen und eine bezahlbare Cyberversicherung abschließen.

Bei der Auswahl eines Managed-SIEM-Services sollte ein Unternehmen auf mehrere Punkte achten: Der Service sollte nicht nur für eine wirksame laufende 24/7 Überwachung sorgen, sondern auch leicht an die IT-Infrastruktur im Unternehmen anpassbar sein. Er sollte zudem klare Handlungsabläufe umfassen, die bei Störungen greifen, einschließlich der NIS-2-konformen Meldung eines Vorfalls. Die Lösung muss per automatisierter Vorfallsanalyse schnell alle nötigen Details liefern, damit das Unternehmen seine Meldefristen einhalten kann.

Die SIEM-Lösung sollte in Europa entwickelt sein und in einer europäischen – idealerweise einer deutschen – Cloud laufen, für die alle einschlägigen BSI- und ISO-Zertifizierungen vorliegen.

So verhandeln deutsche Unternehmen mit ihrem Provider auf Augenhöhe und vermeiden von vornherein Diskussionen um die Compliance der Datenhaltung. Der Servicepartner sollte ein etablierter europäischer Anbieter sein, der Erfahrung mit der Überwachung kritischer IT-Umgebungen vorweisen kann. Auf diese Weise erhält die IT-Infrastruktur eines volkswirtschaftlich wichtigen oder sehr wichtigen Unternehmens einen automatisierten, rund um die Uhr aktiven „Spurhalteassistenten“ – und zugleich eine verlässliche schnelle Alarmierung, sobald die IT doch einmal droht, in den Graben zu fahren.

VORAUSSCHAUENDES FAHREN IST GEFRAGT

Jeder Autofahrer weiß: Wer vorausschauend fährt, statt die Dinge nicht bis zur letzten Sekunde auf sich zukommen zu lassen, reist am sichersten. Ebenso verhält es sich mit der Vorbereitung auf die neuen Verkehrsregeln für die Cybersicherheit. Erfahrungsgemäß entsteht bei der Umsetzung neuer oder aktualisierter Gesetzesvorgaben stets ein Stau durch Unternehmen, die erst „auf den letzten Drücker“ handeln. Selbst wenn einzelne Details der NIS-2-Umsetzung in Deutschland derzeit noch in der Diskussion sind, etwa die persönliche Haftung des Geschäftsführers: Die allermeisten Anforderungen sind allein schon durch die EU-Bestimmungen klar definiert. Verantwortliche sollten deshalb vorausschauend handeln und sich baldmöglich über die Optionen einer zügigen NIS-2-Umsetzung informieren. Denn im Geschäftsleben wie auch bei der Cybersicherheit gilt: Es ist besser, auf der Überholspur freie Fahrt zu haben, als zur Stoßzeit im Stau zu stehen. Managed SIEM aus einer deutschen Cloud macht den Weg frei für die reibungslose Umsetzung der NIS-2-Vorgaben.

ÜBER LOGPOINT

Logpoint ist der Schöpfer einer zuverlässigen, innovativen Plattform für Cybersecurity-Operationen – die Organisationen weltweit befähigt, in einer sich ständig wandelnden Bedrohungswelt erfolgreich zu agieren.

Durch die Kombination anspruchsvoller Technologie und eines tiefen Verständnisses für die Herausforderungen der Kunden stärkt Logpoint die Fähigkeiten der Sicherheitsteams und hilft ihnen, aktuelle und zukünftige Bedrohungen zu bekämpfen.

Logpoint bietet SIEM-, UEBA- und SOAR-Technologien in einer umfassenden Plattform, die Bedrohungen effizient erkennt, falsch-positive Ergebnisse minimiert, Risiken automatisch priorisiert, auf Vorfälle reagiert und vieles mehr.

Mit Hauptsitz in Kopenhagen, Dänemark, und Büros auf der ganzen Welt ist Logpoint ein multinationales, multikulturelles und inklusives Unternehmen.

Für weitere Informationen besuchen Sie www.logpoint.com oder kontaktieren Sie dach@logpoint.com.

www.logpoint.com