ISSN 2198-0527

2/2023

CP CRISIS PREVENTION

Das Fachmagazin für Gefahrenabwehr, Innere Sicherheit und Katastrophenhilfe

INTERVIEW MIT FRANK FRENSER, PRESSESTELLE AMT FÜR FEUERSCHUTZ UND RETTUNGSDIENST DER STADT BONN

SICHERHEIT

Schutz von KRITIS
Drohnen im Einsatz

FEUERWEHR & KATASTROPHENSCHUTZ

Vegetationsbrände
Energieversorgung im Einsatz

KOMMUNIKATION & INFORMATIONSTECHNIK

Alarmierung
BOS-Objektfunk

www.crisis-prevention.de


(Bild: iStock, XH4D)

NIS2 – Der IT-Schutzschirm der EU

Alexander Häußler, Thomas Janz

Die Europäischen Institutionen haben mit der NIS2-Richtlinie die EU-weite Gesetzgebung für die IT-Sicherheit aktualisiert. Seit Anfang 2023 ist diese in Kraft und muss bis Oktober 2024 in nationales Recht überführt werden. Welche Änderungen kommen auf KRITIS-Betreiber zu und wie soll NIS2 die Cyber-Resilienz und Gefahrenabwehr kritischer Infrastrukturen stärken?

NIS stand ursprünglich für „Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz und Informationssystemen in der EU" und hatte zum Ziel, die Mitgliedsstaaten der Europäischen Union (EU) im Bereich der IT-Sicherheit auf Augenhöhe zu bringen und ihre Cyber-Resilienz zu stärken. Das derzeit bestehende IT-Sicherheitsgesetz 2.0 in Deutschland fußt auf der ersten NIS-Richtlinie aus dem Jahr 2016. Es schreibt Mindestanforderungen und Meldepflichten von IT-Sicherheitsvorfällen für 10 KRITIS-Sektoren und drei Kategorien von sogenannten „Unternehmen im besonderen öffentlichen Interesse" (UBI) vor. Dazu gewährte es dem Bundesamt für Sicherheit in der Informationstechnik (BSI) mehr Befugnisse und gab ihm mehr Aufgaben, um die Einhaltung der neuen Gesetzeslage zu ermöglichen. Moniert wurde unter anderem die schwammige Ausgestaltung dessen, ab wann eine Sicherheitslücke offengelegt werden muss. Weitere Kritikpunkte waren das zu niedrig anvisierte, gemeinsame Level an Cyber-Resilienz und die uneinheitliche Einstufung von KRITIS-Betreibern im internationalen Vergleich. Doch auch die Corona-Krise offenbarte neue Schwachstellen in der IT-Sicherheit vieler Einrichtungen und machte ein Nachjustieren der Gesetze erforderlich. Am 14. Dezember 2022 wurde vom Europäischen Parlament und dem Europarat die NIS2-Richtlinie (Richtlinie (EU) 2022/2555) erlassen, die nach Veröffentlichung im Amtsblatt der Europäischen Union im Januar 2023 bis 17. Oktober 2024 von den Mitgliedsstaaten, somit auch von Deutschland, in nationales Recht überführt und ab dem Folgetag angewendet werden muss.

NIS2 verändert die Bemessungsgrundlage für KRITIS-Betreiber und stuft diese nicht länger nach der Menge der Erzeugnisse ein. Zuvor entschied beispielsweise im Trinkwassersektor die aufbereitete Wassermenge in Kubikmetern pro Jahr, welche Unternehmen als Betreiber einer kritischen Infrastruktur betrachtet wurden. NIS2 definiert nun 18 Sektoren und teilt diese wiederum in zwei Gruppen ein: 11 Sektoren gelten als Sektoren mit hoher Kritikalität (Anhang 1 der Richtlinie) und 7 als sonstige kritische Sektoren (Anhang 2). Zwei Kriterien entscheiden, welche Einrichtungen als wesentlich („essential") und welche als wichtig („important") gelten: Die Zugehörigkeit zu einem bestimmten Sektor und die Größe (gemessen an Umsatz und Mitarbeiterzahl).

In Hinblick auf die Größe erweitert die NIS2-Richtlinie den Anwendungsbereich auf KMU (kleine und mittlere Unternehmen). Mittlere Unternehmen beschäftigen 50 bis 250 Mitarbeiter und erzielen entweder einen Jahresumsatz von 10 bis 50 Millionen Euro oder weisen eine Bilanzsumme von höchstens 43 Millionen Euro auf. Kleine Unternehmen beschäftigen weniger als 50 Personen und haben einen Jahresumsatz bzw. eine Jahresbilanz von höchstens 10 Millionen Euro. Kleinstunternehmen haben weniger als 10 Beschäftigte und einen Jahresumsatz bzw. eine Jahresbilanz von unter zwei Millionen Euro. Anzuwenden ist die NIS2 Richtlinie unter anderem auch für Einrichtungen, die auf Grund Ihrer Stellung (bspw. Monopol) oder Tätigkeit (bspw. Domänen-Namen-Registrierungsdienste) den wesentlichen Sektoren zugeordnet werden, unabhängig von Ihrer Größe.

Zu den wesentlichen Einrichtungen gehören Betreiber aus den Sektoren mit hoher Kritikalität, die als mittlere Unternehmen gelten oder die genannten Schwellenwerte für mittlere Unternehmen überschreiten. Zu diesen Sektoren gehören folgende:

- Energie
- Verkehr
- Bankwesen
- Finanzmarktinfrastrukturen
- Gesundheitswesen
- Trinkwasser
- Abwasser
- Digitale Infrastruktur
- Verwaltung von IKT-Diensten (Business-to-Business)
- öffentliche Verwaltung
- Weltraum

Wichtige Einrichtungen umfassen Einrichtungen aus den vorgenannten Sektoren, die nicht die Dimension „Größe" erfüllen, sowie Einrichtungen definierter Art der weiteren kritischen Sektoren:

- Post- und Kurierdienste
- Abfallbewirtschaftung
- Produktion, Herstellung und Handel mit chemischen Stoffen
- Produktion, Verarbeitung und Vertrieb von Lebensmitteln
- Verarbeitendes Gewerbe/Herstellung von Waren
- Anbieter digitaler Dienste
- Forschung

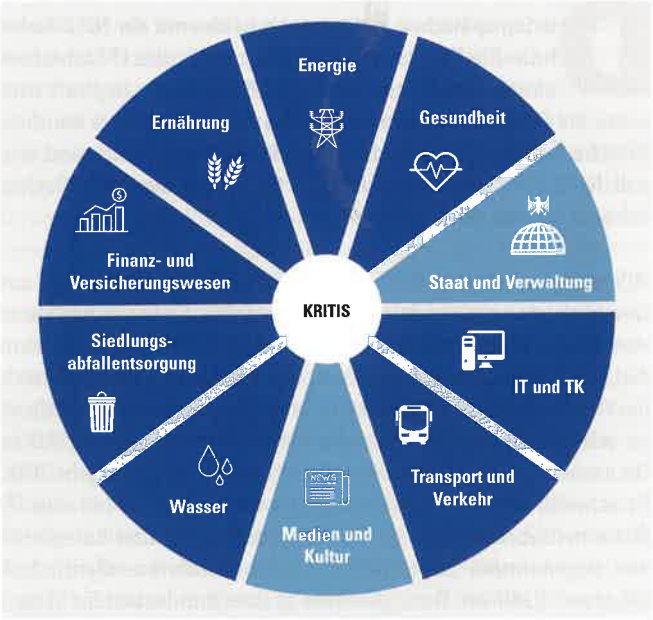
Risikomanagement: Die Checkliste der IT-Sicherheitsmaßnahmen ist lang

NIS2 listet im Wesentlichen zehn verschiedene Themenblöcke aus dem Bereich der Informationssicherheit auf, welche die EU im Rahmen eines widerstandsfähigen Risikomanagements als unabdinglich betrachtet. Auch der oft benannte „Faktor Mensch" – also Risiken durch menschliche Fehlhandlungen und Nachlässigkeiten – soll über grundlegende Verfahren im Bereich des Sicherheitsbewusstseins sowie mit Schulungen im Bereich der Cyber-Sicherheit entschärft werden. Weiterhin schreibt NIS2 verschiedene Sicherheitsrichtlinien, Präventions- und Erkennungsmaßnahmen für Vorfälle sowie die Implementierung von Systemen für Zugangskontrolle und Multi-Faktor-Authentifizierung vor. Außerdem sollen Business Continuity Maßnahmen eingeführt werden, die beispielsweise im Falle einer Verschlüsselung der Daten durch Ransomware den Schaden durch Betriebsunterbrechungen in Grenzen halten sollen. Das beinhaltet auch Backup Management und Disaster Recovery, also die regelmäßige, automatisierte Anfertigung von Kopien der eigenen Daten inklusive der Fähigkeit, diese im Notfall wiederherstellen zu können. Zudem sollen die Leitungsorgane der Einrichtungen mehr in die Pflicht genommen werden, z.B. durch Übertragung der Verantwortung für die Billigung der umzusetzenden Maßnahmen, aber auch durch die Verantwortung für Verstöße gegen die Regelungen der NIS2.

Neben diesen auf die Einrichtungen bezogenen Maßnahmen geht NIS2 auch auf übergeordnete Themen ein. Ergänzend werden im Bereich Einkauf und Beschaffung die Vorschriften zum digitalen Schutz von Lieferketten etabliert, auf die später gesondert eingegangen wird. Nicht zuletzt soll die internationale Kommunikation im Falle eines Hackerangriffs durch die Einführung bzw. Verbesserung von Meldesystemen optimiert werden.

Meldepflicht und IT-Sonderkommandos sind die Erstreaktion bei Cyber-Angriffen

Um auf Cyber-Angriffe reagieren zu können und die Kommunikation zwischen den IT-Fachleuten der einzelnen Länder zu fördern, hat die EU zwei Institutionen ins Leben gerufen: Zum einen die NIS-Kooperationsgruppe, die Mitgliedsstaaten bei der Umsetzung der Maßnahmen der NIS2-Richtlinie unterstützt. Ihr kommt eine beratende und kommunikative Aufgabe zu, die den Wissensaustausch der Staatengemeinschaft zur IT-Sicherheit fördern soll. Im operativen Bereich wird die Gruppe von nationalen Computer Security Incident Response Teams (CSIRTs) unterstützt, die jedes Land gesondert zusammenstellen muss. Nach der Überführung der Richtlinie in nationales Recht bestehen diese Gruppen in Deutschland aus Sicherheitsexperten des BSI, die schwerwiegende Cyber-Attacken auf Anfrage der jeweiligen Betreiber untersuchen und den Betroffenen helfen sollen, wieder auf die Füße zu kommen. Wer die Internetseite des BSI besucht, entdeckt dort schnell den Reiter „IT-Sicherheitsvorfall", unter dem BürgerInnen, Unternehmen und KRITIS-Betreiber solche Vorfälle melden und Unterstützung erhalten können. Diese länderspezifischen Taskforces sollen auf europäischer Ebene in einem CSIRT-Netzwerk zusammenarbeiten und sich über Gefahrenquellen austauschen. Mit Unterstützung der Europäischen Kommission, der ENISA sowie ggf. des CSIRT-Netzwerks, soll die Kooperationsgruppe dann Methoden und organisatorische Aspekte definieren. Dies hat zum Ziel, das Vertrauen und die Zusammenarbeit zu stärken und den Informationsaustausch über bewährte Verfahren zu fördern. Die Teilnahme der CSIRTs an Peer-Reviews ist freiwillig.



(Grafik: TÜV SÜD)

Ergänzend bietet das BSI den KRITIS-Betreibern auf seiner Webseite Informationen zur Prävention etwaiger Zwischenfälle an. Das Meldesystem ist ein Kernelement der IT-Sicherheitspolitik, denn für KRITIS-Betreiber und UBI besteht nicht erst seit NIS2 eine Meldepflicht von Vorfällen. Ein Sicherheitsvorfall gilt als erheblich und meldepflichtig, wenn schwerwiegende Betriebsstörungen, finanzielle Verluste für die Betroffenen oder physischer sowie materieller Schaden an Menschen und Einrichtungen entstehen könnte. Es mag auf den ersten Blick schwer nachvollziehbar sein, wie ein Cyber-Angriff eine Gefahr für Leib und Leben

darstellen kann. Man stelle sich jedoch vor, dass einem Cyber-Kriminellen der Zugriff auf Verkehrssysteme oder die Steuerung der Wasserversorgung gelingt, und schon wird klar, warum der Gesetzgeber die KRITIS-Betreiber abzusichern sucht und warum kritische Infrastrukturen als solche bezeichnet werden.
Wer von einem Sicherheitsvorfall betroffen ist, muss dem BSI oder einem CSIRT innerhalb von 24 Stunden über die Erkennung berichten und einordnen, ob dieser potenziell rechtswidrigen oder böswilligen Ursprungs war und grenzüberschreitende Auswirkungen haben könnte. Innerhalb von 72 Stunden muss eine erste Bewertung samt Einschätzung des Schweregrads und der Konsequenzen erfolgen. Auch ein Abschlussbericht ist spätestens einen Monat nach dem Vorfall bei den genannten Ansprechpartnern abzugeben. Hervorzuheben ist der Umstand, dass CSIRTs in bestimmten Fällen, abhängig von den Auswirkungen des Falls, diesen publik machen können, sofern die Konsequenzen im öffentlichen Interesse liegen oder die Öffentlichkeit betreffen.

Kontrollpflicht für Lieferketten und empfindliche Strafen

Die EU hat erkannt, dass kritische Infrastrukturen nur sicher sind, wenn auch ihre Zulieferer sicher sind. Diverse Beispiele aus aller Welt, sei es Deutschland, die USA oder Ägypten, haben gezeigt, dass es in jeder Lieferkette Nadelöhre geben kann, die im Störfall gesamte Wertschöpfungsketten zum Erliegen bringen können – mit weitreichenden Folgen. Diese Störungen können, wie im Fall des havarierten Schiffes im Suezkanal im Jahr 2021, die gesamte Weltwirtschaft belasten und zeigen die Empfindlichkeit des komplexen Netzes globaler Lieferketten auf.
Die Cyber-Resilienz einer Lieferkette ist immer abhängig von ihrem schwächsten Glied – das ist auch bei KRITIS-Einrichtungen nicht anders. Auch diese sind zum einen auf Lieferketten angewiesen und zum anderen selbst Teil von Lieferketten. Diesen Tatsachen hat NIS2 Rechnung getragen. So ist eine der verpflichtenden Maßnahmen, die von den wesentlichen und wichtigen Einrichtungen umzusetzen sind, die Überprüfung der eigenen Lieferkette. Die Detaillierungen zu diesem Punkt sind nicht sehr umfangreich, so dass es den Einrichtungen selbst obliegt, die Angemessenheit der getroffenen Maßnahmen in diesem Bereich zu bewerten. Als Anhaltspunkte nennt die Richtlinie, dass auch die Beziehungen zwischen den Einrichtungen betrachtet werden sollen und dass die Gesamtqualität in Bezug auf die Cyber-Sicherheit ebenso zu bemessen ist wie ein ggf. vorhandener Einwicklungsprozess. Des Weiteren eröffnet NIS2 die Möglichkeit, dass gewisse kritische Lieferketten – die durch die Europäische Kommission nach Rücksprache mit der Kooperationsgruppe und der ENISA festgelegt werden – einer koordinierten Risikobewertung unterzogen werden. Die Risikobewertung ist für alle Einrichtungen verbindlich, die diese Lieferkette nutzen.
Die Strafmaßnahmen für Nachlässigkeiten bei der Umsetzung der Gesetzesvorgaben sind alles andere als harmlos – sie sollen abschrecken. Abhängig davon, ob eine KRITIS-Einrichtung als wesentlich oder wichtig eingestuft wurde, fallen die Sanktionen unterschiedlich aus. Als wesentlich betrachtete Einrichtungen müssen mit Strafen bis zu einer Höhe von mindestens zehn Millionen Euro oder zwei Prozent des weltweiten Umsatzes rechnen, sofern sie die geforderten Maßnahmen nicht umgesetzt haben. Als wichtig kategorisierte Einrichtungen haben eine Höchststrafe von mindestens sieben Millionen Euro oder 1,4 Prozent des weltweiten Umsatzes zu erwarten. Die Mitgliedsstaaten haben darüber hinaus die Möglichkeit, weitere Sanktionen zu erlassen, die wirksam, verhältnismäßig und abschreckend ausfallen müssen. Es darf darüber hinaus nicht vergessen werden, dass das BSI dazu befugt ist, unangekündigte Kontrollen, Stichproben und Sicherheitsprüfungen mit unabhängigen Experten in regelmäßigen Abständen durchzuführen. Zusätzlich können sie Nachweise über die Erfüllung festgelegter Standards einfordern und bei gegebenem Anlass eine Akten- und Dateneinsicht erhalten. Daher ist besonders der Geschäftsleitung angeraten, die Richtlinie rechtzeitig und bestenfalls vor der Überführung in nationales Recht zeitnah umzusetzen – weil sie im schlechtesten Falle für Versäumnisse bei der Implementierung haftbar gemacht wird.

Zwei gute Gründe für die frühzeitige Zertifizierung

Die NIS2-Richtlinie gibt allen EU-Mitgliedsstaaten die Möglichkeit, zertifizierte IKT-Produkte und -Dienste bereits im Ausschreibungsverfahren von potenziellen Anbietern zu verlangen. Obwohl die Zertifizierungen selbst nicht verpflichtend sind, werden alle EU-Länder zumindest angehalten, Normen zu erlassen, welche die IT-Sicherheitsgefahren für wesentliche und wichtige Einrichtungen möglichst geringhalten. Betroffene sollten die Tatsache, dass Zertifizierungen nicht rechtlich bindend sind, nicht auf die leichte Schulter nehmen. Zum einen kann es durchaus sein, dass das unumgängliche „IT-Sicherheitsgesetz 3.0" solche Zertifizierungen und regelmäßige Audits vorschreiben wird, zum anderen ist eine Rundum-Überprüfung der Konformität hauseigener IT-Systeme mit den aktuellen Sicherheitsstandards ohnehin uneingeschränkt zu empfehlen. Natürlich sind die Strafmaßnahmen empfindlich, ein viel wichtigerer Anreiz sollte jedoch die aktuelle Gefahrenlage und die Tatsache sein, dass Cyber-Kriminellen die Wichtigkeit von KRITIS überaus bewusst ist. Der Gesetzgeber betreibt hier kein Spiel mit der Angst, im Gegenteil – Betreiber kritischer Infrastrukturen vermeiden ein Spiel mit der Zeit, wenn sie sich bereits frühzeitig und vor Oktober 2024 damit befassen, ihre Lieferketten und IT-Systeme resilient zu gestalten. Audits sind dabei keine Schikane, sondern ein zuverlässiger Weg hin zu einer zeitgemäßen Widerstandsfähigkeit. CP

Alexander Häußler
Global Product Performance Manager IT
E-Mail: Alexander.Haeussler@tuvsud.com

Thomas Janz
Product Compliance Manager IT Standards
E-Mail: Thomas.Janz@tuvsud.com
TÜV SÜD Management Service GmbH
Westendstraße 199
80686 München / Munich