„Ein **Schubs** in die richtige Richtung“

Vor dem Inkrafttreten der Netz- und Informationssicherheitsrichtlinie **NIS2** ist noch einiges unklar.

VON KATIA MEYER-TIEN UND TOM WEINGÄRTNER

Unterschätzen sollte man die Gefahr nicht: „Wenn Sie Informationssicherheit bislang noch stiefmütterlich behandelt haben“, sagt Bernhard Schiemann, Teamleiter Cyber Security beim IT-Consulting-Unternehmen BTC, „dann können Sie in dieser Liga als Verteidiger gar nicht mitspielen. Die Angreifer sind nicht nur technisch versiert, sondern die sind auch schnell. Die sind irre schnell.“

Mehr als 2.000 neu bekannt gewordene Schwachstellen in Softwareprodukten, davon 15 Prozent kritisch, zählte das Bundesamt für Sicherheit in der Informationstechnik (BSI) 2023 pro Monat, ein Zuwachs von 24 Prozent im Vergleich zum Vorjahr. „Und von der Bekanntgabe der Schwachstelle dauert es oft nur drei, vier Stunden, bis Angreifer versuchen, genau diese Schwachstelle in der Infrastruktur zu finden“, sagt Schiemann. „Da haben Sie nicht viel Zeit.“

Und Schwachstellen in Softwareprodukten sind nur eines von vielen Einfallstoren. Eine Viertelmillion neue Schadprogrammvarianten wurden 2023 durchschnittlich an jedem Tag gefunden, insgesamt 68 erfolgreiche Ransomware-Angriffe wurden bekannt und täglich durchschnittlich rund 776 E-Mails mit Schadprogrammen allein aus Regierungsnetzen abgefangen, so der BSI-Bericht zur Lage der IT-Sicherheit in Deutschland 2023, der zu dem Schluss kommt: Die Bedrohung im Cyberraum ist so hoch wie nie zuvor. Und: 74 Prozent der Cyberattacken in der Europäischen Union zielten im Jahr 2023 auf kritische Infrastrukturen ab, wie es im „X-Force Threat Intelligence Index 2024“ von IBM heißt.

Keine gemeinsame Strategie

Auch in der EU hat man erkannt, dass sich nicht zuletzt durch die Covid-Krise „die Bedrohungslandschaft erweitert“ hat, wie es aus Brüssel heißt: Die europäische Wirtschaft setze verstärkt auf digitale Lösungen und sei immer stärker vernetzt. Störungen blieben immer weniger auf eine Firma oder einen Sektor begrenzt. Schon 2020 kam die EU-Kommission bei der Überprüfung der 2016 verabschiedeten „Netz- und Informationssicherheitsrichtlinie“ (Network and Information Security Directive NIS) zu dem Ergebnis: Viele Unternehmen waren nur unzureichend gegen Cyberrisiken gesichert, unter den Mitgliedstaaten gab es kein gemeinsames Verständnis der Bedrohungen im Cyberraum und keine gemeinsame Strategie, sich dagegen zu schützen. Sie schlug deswegen eine neue Richtlinie, NIS2, vor, die im November 2022 verabschiedet wurde. Diese muss bis Oktober 2024 von den Mitgliedstaaten in nationales Recht umgesetzt werden.

In Deutschland sorgt die Richtlinie derzeit noch für viel Unsicherheit, was auch daran liegt, dass unklar ist, wie sie hierzulande umgesetzt wird. Ein erster Entwurf für ein entsprechendes Gesetz wurde im vergangenen Jahr diskutiert, nun ist seit Anfang Mai der „Referentenentwurf eines Gesetzes zur Umsetzung der NIS2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung“ im Umlauf. Das fertige Gesetz ist wohl nicht vor Anfang 2025 zu erwarten.

Richtlinie verlangt Strategie

Die Richtlinie verlangt von den Mitgliedstaaten, eine Cybersicherheitsstrategie zu entwickeln und nationale Sicherheitsgruppen (Computer Security Incident Response Teams CSIRT) zu bilden, die für den Umgang mit Störungen im Cyberraum zuständig sind. Die von der Richtlinie erfassten Unternehmen müssen bestimmte Anforderungen erfüllen und Sicherheitsmaßnahmen ergreifen. Störungen ab einem bestimmten Umfang müssen den Behörden gemeldet werden.

Schon jetzt klar ist dabei vor allem eines: Der Kreis der betroffenen Unternehmen wird größer. Die NIS2 weitet die bislang geltenden Anforderungen für Unternehmen der kritischen Infrastruktur auch auf „mittlere Unternehmen“ und auf öffentliche und private Einrichtungen „von besonderer Bedeutung“ aus. Dabei haben die Mitgliedstaaten einen gewissen Spielraum, solche Einrichtungen oder Unternehmen auszuweisen. Die Vorstellung der EU: Unternehmen bestimmter Branchen – darunter auch der Energiebranche – ab 50 Mitarbeitenden oder mindestens 10 Millionen Euro Jahresumsatz und Jahresbilanzsumme sollen zum Kreis derer gehören, die geeignete Sicherheitsmaßnahmen ergreifen und die zuständigen nationalen Behörden über schwerwiegende Vorfälle informieren müssen. Dafür erhalten die Aufsichtsbehörden zusätzliche Kompetenzen und vor allem stärkere Instrumente, um die Einhaltung der Richtlinie durchzusetzen. Zum Beispiel dürfen sie Geldbußen bis zu 10 Millionen Euro oder 2 Prozent des weltweiten Umsatzes verhängen.

„Bumerang für Cybersicherheit“

Dass die Einstufung künftig nicht an der tatsächlichen Relevanz für die Versorgungssicherheit, sondern anhand der Betriebsgröße erfolgen soll, gehört zu den Regelungen, die Branchenvertreter am stärksten kritisieren.

VKU-Hauptgeschäftsführer Ingbert Liebing beispielsweise warnt davor, dass das Gesetz auf diese Weise im schlimmsten Fall zum „Bumerang für die Cybersicherheit“ werden könnte – dann nämlich, wenn in größeren Unternehmen Ressourcen für IT-Sicherheit über das gesamte Unternehmen allokiert werden müssten, statt zielgerichtet in die wirklich kritischen Bereiche zu fließen: „Wir bitten die Bundesregierung zu prüfen, ob Mitarbeiterzahl und Umsatz wirklich sinnvolle Kriterien sind.“

Auch der BWE sieht in seiner Stellungnahme zum Referentenentwurf noch „Klärungsbedarf zu einer Reihe von Punkten“, fordert klare und praxistaugliche Regelungen und warnt insbesondere vor neuen bürokratischen Hemmnissen für Betreibergesellschaften von Windenergieanlagen und Windparks, deren Partnerunternehmen oder verbundene Unternehmen.

Betroffene nicht informiert

Für Unsicherheit in der Branche sorgt auch, dass betroffene Unternehmen nicht informiert werden, sondern ihre Betroffenheit selbst herausfinden müssen. Eine ganze Reihe von Anbietern hat daher bereits „Betroffenheitschecks“ entwickelt, darunter auch BTC. „Klar ist: Es betrifft jetzt auch Unternehmen, die bislang eher unter dem Radar fliegen. Die bisher gesagt haben: Wir sind kleiner, uns betrifft das nicht. Für diese ist die Betroffenheitsfeststellung manchmal ein Augenöffner: Oh, jetzt müssen wir doch“, sagt BTC-Experte Bernhard Schiemann.

Allerdings seien viele Unternehmen aus der Energiewirtschaft ohnehin schon sehr gut aufgestellt – auch weil viele Anforderungen für sie schon länger gelten. „Unternehmen, die bereits über ein zertifiziertes ISMS (Information Security Management System) verfügen, würde ich vorsichtig sagen: Lasst das auf euch zukommen, das wird euch nicht aus der Bahn werfen.“ Schließlich seien ISMS ohnehin Systeme, die sich den Anforderungen entsprechend laufend weiterentwickeln.

IT-Sicherheit ist Chefsache

Von etwa 30.000 neu betroffenen Unternehmen deutschlandweit in allen Branchen gehen Experten momentan aus. Etwa 1.000 davon verortet Schiemann im Umfeld der Energiewirtschaft. „Viele denken vielleicht, da kommt von ganz oben wieder ein Regularium auf mich runtergepurzelt, jetzt muss ich noch eins umsetzen“, sagt Schiemann. Angesichts der zunehmenden Risiken sieht er die NIS2-Richtlinie aber eher als „Schubs in die richtige Richtung“, denn: „Die Bedrohung bleibt und sie verändert sich und dem trägt auch die NIS2-Richtlinie Rechnung.“

Dementsprechend rät er auch kleinen oder sehr kleinen Unternehmen dazu, funktionierende Systeme zur Informationssicherheit einzuführen. Und die IT-Sicherheit zur Chefsache zu machen: „Man kann sich nicht wegducken, bloß weil man dem Hausmeister einen Besen gekauft hat und der sollte Schnee räumen. Man muss das auch noch kontrollieren. Dem Geschäftsführer obliegt die Kontrolle der Abwehr gegen Angriffe.“

Dass all das angesichts der vielfältigen Anforderungen, denen sich die Energiewirtschaft momentan gegenübersieht, und angesichts des allgemeinen Fachkräftemangels keine einfache Aufgabe ist, dessen ist sich der Experte wohl bewusst. Er rät zu Kooperationen, beispielsweise bei Lieferantenaudits: „Wenn man als kleines Stadtwerk vielleicht Schlüssellieferanten hat und weiß, Nachbarstadtwerke müssen diesen Lieferanten auch auditieren: Da kann man sich ja zusammentun.“

Denn letztlich führt – auch ganz unabhängig davon, wie die konkreten Ausführungen des Umsetzungsgesetzes letztlich lauten und wer tatsächlich von den neuen Bestimmungen betroffen ist – auch für die kleinsten Unternehmen kein Weg an der Entwicklung einer Cybersecurity-Strategie vorbei. E&M

ENERGIE & MANAGEMENT
ZEITUNG FÜR DEN ENERGIEMARKT