FACTORY

MELZER PR GROUP since 1989
CORPORATE COMMUNICATIONS

NIS2 Cybersicherheit: Handschellen oder Notwendigkeit? (1/2)

FactoryAusgabe 02/2024 | Seite 36, 37 | 17. April 2024
Auflage: 8.030 | Reichweite: 23.287

Melzer PR Group

Im Fokus
Digitalisierung

C_IFWK/PEROUTKA

V. l. Martin Krumböck (T-Systems), Robert Lamprecht (KPMG), Isabella Mader (Excellence Research), Gerald Schremser (Prinzhorn Gruppe), Christina Wilfinger (SAP), Rudolf J. Melzer (IFWK)

Experten über die neue Richtlinie

NIS2 Cybersicherheit: Handschellen oder Notwendigkeit?

Die EU-Richtlinie NIS2 schreibt strenge Maßnahmen zur Gewährleistung der Cybersicherheit vor und muss in Österreich bis Oktober 2024 von 9.000 großen Firmen und vielen Mittelständlern umgesetzt werden. Die rasche und professionelle Umsetzung der notwendigen Sicherheitsmaßnahmen stand im Mittelpunkt einer Expertendiskussion des Internationalen Forums für Wirtschaftskommunikation.

KPMG-Partner Robert Lamprecht, der auch in der Vorsitzführung der Arbeitsgruppe für die NIS2-Risikomanagementmaßnahmen tätig ist, plädiert dafür, Cybersicherheit nicht nur als technische Aufgabe zu betrachten, sondern auch organisatorische Faktoren und den Menschen im Mittelpunkt einzubeziehen: „Führungskräfte haben es selbst in der Hand, sich mit Cybersicherheitsmaßnahmen in einem regulierten Umfeld oder mit den schmerzhaften Folgen von Cyberattacken bei Versäumnissen auseinanderzusetzen."

In Österreich gilt aktuell das NIS-Gesetz aus dem Jahr 2016, das Anforderungen an die Cybersicherheit in gesellschaftlich wichtigen Bereichen spezifiziert. Mit NIS2 wird die Zahl der betroffenen Unternehmen kräftig erweitert – es betrifft 3.000 bis 9.000

FACTORY

MELZER PR GROUP since 1989
CORPORATE COMMUNICATIONS

NIS2 Cybersicherheit: Handschellen oder Notwendigkeit? (2/2)

FactoryAusgabe 02/2024 | Seite 36, 37 | 17. April 2024
Auflage: 8.030 | Reichweite: 23.287

Melzer PR Group

große Firmen und den Mittelstand. Darunter fallen sowohl wesentliche (u. a. Unternehmen im Trinkwasserbereich und Energielieferanten) als auch wichtige (u. a. aus dem Lebensmittelsektor) Unternehmen. Für sie gelten künftig ein verpflichtendes Risikomanagement und Meldevorschriften bei Sicherheitsvorfällen. Viele Betroffene dürften sich der Tragweite noch nicht bewusst sein, obwohl bei Vergehen Strafen von bis zu zehn Millionen Euro oder zwei Prozent des Konzernumsatzes drohen – für die Führungskräfte auch persönlich haftbar gemacht werden können.

Auch für Partnerfirmen und Lieferanten relevant

Laut einer aktuellen Studie von KPMG gemeinsam mit dem Kompetenzzentrum Sicheres Österreich haben sich Cyberangriffe zuletzt innerhalb von zwölf Monaten mehr als verdreifacht. 12 Prozent der in der Studie befragten heimischen Unternehmen hatten bei Sicherheitsvorfällen Schäden von mehr als eine Million Euro verzeichnet, mehr als die Hälfte Schäden von mindestens 100.000 Euro. Dabei wird meist die am schwächsten abgesicherte Firma in Lieferketten betroffen – daher sei NIS2 auch für die Partner und Lieferanten der großen Unternehmen relevant. „Risiken, die andere eingehen, sind auch meine Risiken", spricht Lamprecht von einer neuen Verantwortung in einer vernetzten Wirtschaft.

Philipp Töbich verantwortet mit seinem Team Sicherheitsthemen bei SAP in Europa und international – und steht damit im Rampenlicht der Weltwirtschaft. SAP-Kunden generieren 87 Prozent des globalen Handelsvolumens. „Das Thema der Netz- und Informationssicherheit gibt es nicht erst seit gestern", berichtet der Experte von fünfzigjähriger Erfahrung des Softwareherstellers mit dem Schutz von Daten. Töbich betrachtet die NIS2 grundsätzlich positiv. Gerade größere Unternehmen hätten bereits enorme Ressourcen in die Sicherheit gesteckt. Jetzt sei es wichtig, eine möglichst harmonische Gesetzgebung in Europa und deren Umsetzung in der Breite zu erreichen. Denn die Gefahren sind mit den geopolitischen Eskalationen in jüngster Zeit nicht weniger geworden.

Unabhängiger Nachweis wäre wichtig

Gerald Schremser, CISO bei der Prinzhorn Gruppe, lieferte einen Einblick in die Praxis und wünscht sich auch künftig die Möglichkeit der eigenen Gestaltung von IT-Sicherheit. Er prüft mit seinem Team mit Gap-Analysen den Statusquo und Umsetzungsmöglichkeiten bei Sicherheitsthemen. Offen ist für den CISO die Frage, wie bei den Berichtspflichten künftig mit zu erwartenden gehäuften Anfragen in der Lieferkette umgegangen wird. Es würden jedes Jahr hunderte Anfragen zu Sicherheitsbelangen drohen. „Hier würde ich mir einen unabhängigen Nachweis der Erfüllung der Pflichten nach NIS2 wünschen, den unsere Partner für ihre Meldungen an die Behörde nutzen können", so Schremser. «

NIS2 im Faktencheck

Vorsicht vor Falschinformationen!

Die Verunsicherung der Unternehmen wächst, je näher der Termin für die Umsetzung der NIS2-Richtlinie durch die EU-Mitgliedstaaten rückt. Die vielfach unklare NIS2-Richtlinie führt zu einer Goldgräberstimmung unseriöser Anbieter.

Mythos 1:
„NIS2 betrifft alle Wirtschaftsakteure, die wesentliche Dienste anbieten, einschließlich KMU."

Falsch! Es ist richtig, dass die NIS2 wesentliche und wichtige Anlagen kennt. Für die meisten Unternehmen gilt die Richtlinie jedoch nur, wenn sie nach der Definition der Europäischen Kommission mindestens die Größe mittlerer Unternehmen erreichen. Kleinst- und Kleinunternehmen sind regelmäßig ausgenommen.

Mythos 2:
„In NIS2 werden Regeln für neue Technologien wie künstliche Intelligenz und das Internet der Dinge festgelegt."

Falsch! Für den Einsatz von IoT-Geräten oder KI-Systemen im Unternehmen gelten selbstverständlich die Anforderungen von NIS2. NIS2 enthält hierfür jedoch keine speziellen Regelungen. Allerdings hat die EU mit der Funkanlagenrichtlinie, die bereits in Kraft getreten ist, sowie der KI-Verordnung und dem Cyber Resilience Act, die sich im Gesetzgebungsverfahren befinden, umfangreiche Regelungen für die genannten Bereiche getroffen.

Mythos 3:
„Ich muss ein Produkt kaufen, um NIS2 zu erfüllen."

Falsch! Von einigen Anbietern wird der Eindruck erweckt, dass die Anforderungen der NIS2-Richtlinie allein durch die Inanspruchnahme bestimmter Dienstleistungen oder den Erwerb von Softwareprodukten erfüllt werden können. Ein ganzheitlicher Ansatz, der neben einer umfangreichen Dokumentation und technischen Maßnahmen auch organisatorische Maßnahmen beinhaltet, ist jedoch für die Umsetzung von Risikomanagementmaßnahmen erforderlich. Wenn der Kauf eines einzelnen Produktes als ultimative Lösung angepriesen wird, ist eine gesunde Skepsis angebracht.