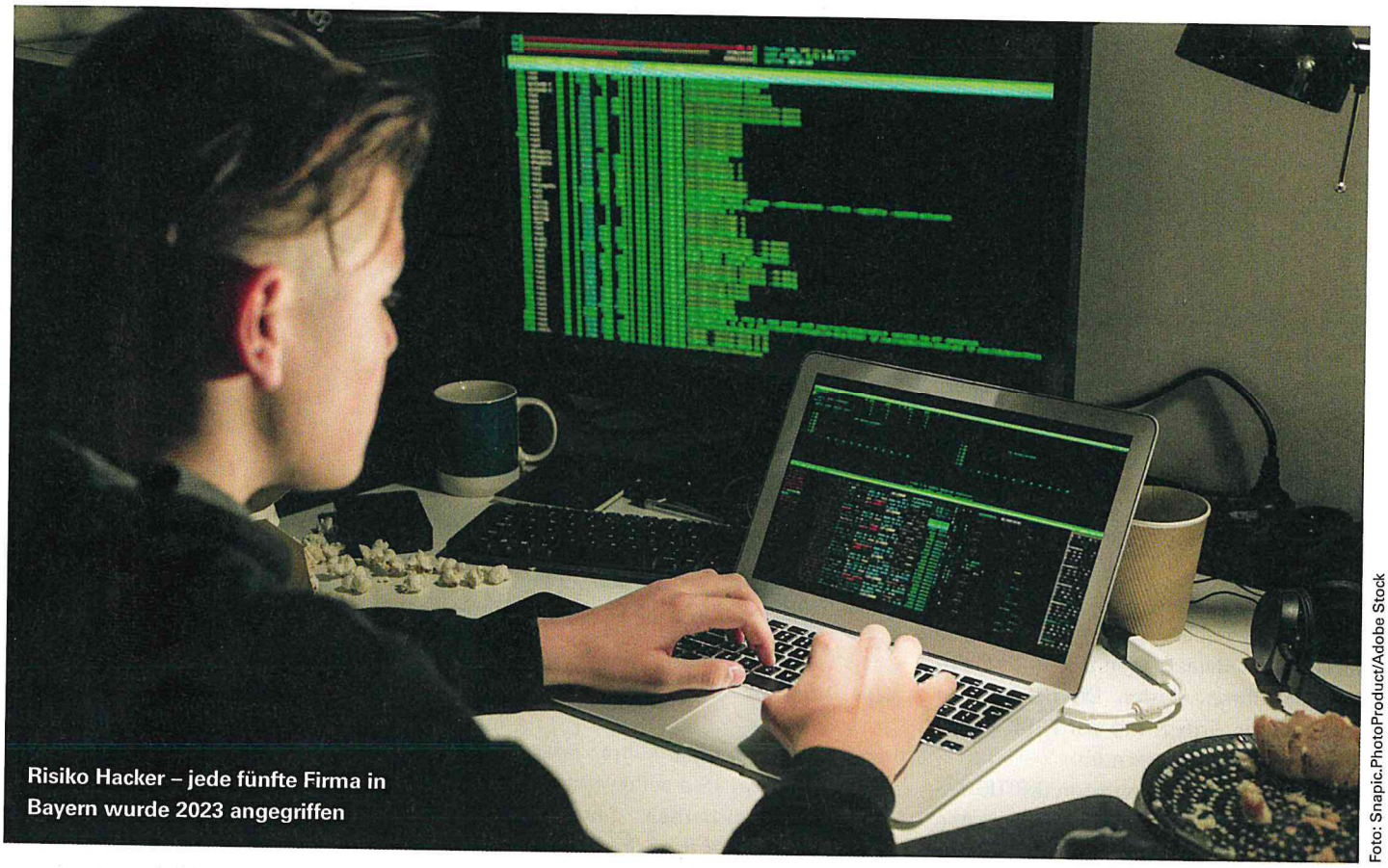

Risiko Hacker – jede fünfte Firma in Bayern wurde 2023 angegriffen

Foto: Snapic.PhotoProduct/Adobe Stock

Cyberkriminelle abwehren

Ab 18. Oktober 2024 gilt die neue NIS2-Richtlinie. Mit ihr will die Europäische Union die Cybersicherheit stärken. Was die neuen Regeln für Unternehmen bedeuten.

Von Gabriele Lüke

Die freundliche Mail kam vom Chef höchstpersönlich. Sie bot dem neuen Mitarbeiter als Willkommensgeschenk wertvolle Gutscheine an – angeblich. »Tatsächlich versteckte sich dahinter der dreiste Versuch, in unser IT-System einzudringen und es auszuspähen«, berichtet Muamer Babajic, Geschäftsführer der Masterwerk GmbH in München. Das Unternehmen liefert der Automobilindustrie und Produktionsbetrieben Automatisierungslösungen zu. »Ein Klick auf den integrierten Link hätte genügt und der Hacker wäre in unserem System gewesen. Aber wir haben den Cyberangriff erkannt und abgewehrt.«

Babajic berichtet von der IT-Attacke deshalb so offen, weil er andere Unternehmen warnen und sensibilisieren möchte: »Cybersicherheit ist bei uns weit oben auf der Tagesordnung, wir schulen unsere Beschäftigten regelmäßig, ergreifen technische Maßnahmen. Und doch sind wir, wie die Episode zeigt, nicht automatisch vor potenziellen Angriffen gefeit und müssen wachsam bleiben.«

2023 ist die Zahl der Straftaten im Bereich Cyberkriminalität erneut gestiegen. Laut der IHK Digitalisierungsumfrage ist jedes fünfte Unternehmen in Bayern Opfer eines Cyberangriffs geworden. Auch die EU hat reagiert. Sie hat die aus dem Jahr 2016 stammende Richtlinie zur Netzwerk- und Informationssicherheit (NIS) verschärft: Mit der NIS2 (EU-Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der gesamten Union) will sie eine zeitgemäße und europaweit harmonisierte Abwehr von Cybergefahren schaffen.

Die NIS2 muss von den Mitgliedstaaten bis zum 17. Oktober 2024 in nationales Recht umgesetzt sein. Dafür bereitet die Bundesregierung derzeit das NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) vor. Ob es rechtzeitig fertig wird, ist offen: Anfang Mai 2024 wurde ein Referentenentwurf

Foto: privat

veröffentlicht und die Anhörung dazu gestartet, an der auch die IHK teilnimmt. »Dennoch müssen die Unternehmen ab dem 18. Oktober 2024 gesetzeskonform handeln – dann wohl zunächst auf Basis der Richtlinie selbst«, betont Sophie Haack, Projektmanagerin der Transferstelle Cybersicherheit im Mittelstand in Magdeburg.

Direkte Adressaten der Richtlinie sind Einrichtungen, bei denen IT-Störungen zu erheblichen Belastungen des Allgemeinwesens führen würden. Die EU hat den Kreis dieser Firmen mit der NIS2 erweitert und fasst darunter nun:

- Betreiber kritischer Anlagen (KRITIS-Betreiber, sie waren bereits die Adressaten der ersten NIS) sowie »besonders wichtige« Einrichtungen von hoher Kritikalität mit mindestens 250 Mitarbeitenden oder mehr als 50 Millionen Euro Jahresumsatz oder 43 Millionen Euro Jahresbilanzsumme. Nach Sektoren sind dies Energie, Transport, Verkehr, Finanzen, Versicherungen, Gesundheit, Wasser, Abwasser, Informationstechnologie, Telekommunikation und Weltraum.
- »Wichtige« Einrichtungen in sonstigen kritischen Sektoren mit mindestens 50 Mitarbeitenden oder mehr als zehn Millionen Euro Jahresumsatz oder zehn Millionen Euro Jahresbilanzsumme. Hier sind es die Branchen Post, Kurierdienste, Siedlungsabfallentsorgung, Chemie, Lebensmittel, verarbeitendes Gewerbe, digitale Forschung oder Vertrauensdienste.
- Spezielle Einrichtungen zum Beispiel für Domains, DNS, qualifizierte Vertrauensdienste, Telekommunikationanbieter können ebenso als »besonders wichtig« beziehungsweise »wichtig« gelten.

Insgesamt fallen 30.000 Unternehmen in Deutschland unter NIS2. Doch damit nicht genug. Die EU verpflichtet die 30.000 direkt Betroffenen zudem, ihre Lieferketten zu untersuchen. »Sie sollen nicht nur die eigene Cybersicherheit gewährleisten, sondern auch die ihrer Partner mitkontrollieren«, nennt Expertin Haack einen ersten inhaltlichen Knackpunkt der Richtlinie. »Auch Betriebe, die auf den ersten Blick nicht unter die NIS2 fallen, sollten daher vorsorglich prüfen, ob sie durch Auftraggeber und Kunden indirekt betroffen sein könnten.« Außerdem fordert die EU den Allgefahrenansatz. Das heißt: Die IT soll nicht nur vor Cyberangriffen, sondern zum Beispiel auch vor Naturkatastrophen geschützt werden.

Praktisch verlangt der EU-Gesetzgeber von betroffenen Unternehmen, die Geschäftskontinuität auch im Worst Case zu gewährleisten, dafür Risikomanagementsysteme zu installieren, Registrierungs-, Nachweis- und Unterrichtungspflichten nachzukommen und technische sowie organisatorische Maßnahmen zu ergreifen.

Ein erheblicher Cybervorfall muss innerhalb von 24 Stunden mit einer Frühwarnung einer dafür geplanten Meldestelle angezeigt werden. »Das BSI kann zudem stichprobenweise prüfen, wie ein Unternehmen sich schützt«, ergänzt Expertin Haack. »Sind die Maßnahmen nicht ausreichend, gibt es hohe Strafen. Die Geschäftsführung steht in der Haftung.«

Bernhard Kux, IT-Referent der IHK für München und Oberbayern, hält die Anforderungen der Richtlinie grundsätzlich für sinnvoll: »Die NIS2 ist ein guter Hebel für mehr Sensibilisierung und praktische Cybersicherheit.« Er betont aber auch: »Für die Umsetzung braucht es Augenmaß.«

Im ersten Schritt sollten Firmen prüfen, ob sie von der neuen Richtlinie betroffen sind. »Die Betriebe müssen selbst eruieren, ob sie unter NIS2 fallen«, sagt Thomas Neeff, Geschäftsführer der TEN Information Management GmbH in Höhenkirchen-Siegertsbrunn. »Das BSI informiert sie nicht darüber.« Eine Herausforderung sei die genaue Zuordnung zu den Sektoren.

Neeff empfiehlt, in die EU-NIS2 und den Referentenentwurf der deutschen NIS2-Umsetzung zu schauen: Die Anhänge 1 und 2 listen alle Sektoren detailliert auf, in Paragraf 28 ist die Betroffenheit geregelt. »Auch die Lieferkette oder die indirekte Betroffenheit sollten an dieser Stelle mitbedacht werden«, so der Experte.

Anschließend gilt es, organisatorische Strukturen zu schaffen. Expertin Haack von der Transferstelle Cybersicherheit rät: »Die NIS2 sollte ganz oben im Unternehmen aufgehängt werden. Die Geschäftsführung muss überzeugt dahinterstehen – und dann mindestens eine Person be-

nennen, die sich in der Praxis speziell um sie kümmert.« Dies sollte nicht der Datenschutzbeauftragte oder IT-Administrator sein.

Es folgt die Bestandsaufnahme. Es gibt kaum Unternehmen, die bisher überhaupt keine IT-Sicherheitsmaßnahmen ergriffen haben – zumindest ein regelmäßiges Back-up von Daten gehört heute zum Standard. »Einige Unternehmen sind zudem durch die ISO 27001 oder den IT-Grundschutz gerüstet«, sagt IT-Fachmann Neeff. »Darauf kann man aufbauen.«

Bei der Konkretisierung der Maßnahmen ist dem Experten vor allem die Sensibilisierung der Mitarbeitenden ein Anliegen. »Nicht nur, weil die NIS2 es verlangt – menschliche Schwäche und Manipulierbarkeit sind die häufigsten Einfallstore für Cyberkriminelle«, so Neeff. Inzwischen gebe es viele Schulungsmöglichkeiten, auch online. Bei den technischen Maßnahmen seien die Multifaktorauthentifizierung oder ein Log-in-Verfahren nach dem Single-Sign-On-Verfahren (SSO) ein guter Standard.

Beim Notfallplan sollten Unternehmen unbedingt die Worst Cases durchspielen und dabei möglichst alle Gefahren für die IT-Sicherheit einbeziehen – vom Hacker bis zum Extremwetter. Erst dann lasse sich ein Maßnahmenplan zur Risikovorsorge finalisieren und die Geschäftskontinuität angemessen sichern, sagt Neeff. »Und dann gilt es, die Pläne immer wieder zu aktualisieren und anzupassen und die Abläufe regelmäßig zu üben.« Passiert dennoch etwas, erwartet das BSI schnell eine Meldung. »Hier rate ich, besser einmal zu viel als zu wenig zu melden«, so der Experte.

Und wie gehen Unternehmen in der Praxis mit den neuen Vorgaben um? Die MTG-Kommunikations-Technik GmbH mit Stammsitz in München prüft aktuell, inwieweit sie von der NIS2 betroffen ist. »Wir arbeiten seit jeher in einer sehr sicherheitssensiblen Branche, insofern ist auch die Cybersicherheit für uns schon immer ein Thema – wir beschäftigen uns regelmäßig damit«, sagt Geschäftsführerin Silvia Keitel.

Erst kürzlich hat das Unternehmen wieder einen ausführlichen Vulnerability-Scan in seinem Netzwerk durchgeführt, die Mitarbeiter in Webinaren für Cybersicherheit sensibilisiert und sie durch eine unangekündigte Phishing-Simulation gezielt herausgefordert. »Auf Schulungen legen wir viel Wert«, sagt Keitel. »So hat unser Team die Simulation auch gut gemeistert, wir waren sehr zufrieden.«

Bei technischen Maßnahmen setzt MTG neben der klassischen Antivirensoftware auf eine umfassende »24/7 Managed Service Extended Detection and Response Lösung«. Sie beobachtet rund um die Uhr die Telemetriedaten und erkennt Anomalien sofort. Eine weitere wichtige Maßnahme ist ein mehrschichtiges Back-up-Konzept. Einen Notfallplan für Worst-Case-Szenarien hat die MTG ebenfalls in der Schublade. Keitel: »Wir sind auf jeden Fall auf die NIS2 vorbereitet.«

Unternehmer Babajic weiß bereits, dass er durch seine Kunden indirekt von der NIS2 betroffen sein wird. Er hat schon vor längerer Zeit einen Beauftragten für Cybersicherheit eingesetzt und mit ihm einen Notfallplan aufgestellt. Technische Maßnahmen der Wahl sind vor allem die Zwei-Faktor-Authentifizierung (2FA), der Schutz vor Datenverlust via Data Loss Prevention (DPL) sowie die Überwachung und die Reaktion auf potenzielle Angreifer mithilfe künstlicher Intelligenz.

»Der Schwerpunkt unseres Sicherheitskonzepts liegt aber eindeutig auf Schulungsmaßnahmen«, sagt Babajic. »Ein hoch sensibilisiertes Team ist der beste Schutz gegen Cyberkrimininalität.« Außerdem legt er bei allen Maßnahmen immer wieder nach. »Wir werden als Unternehmen zunehmend bekannter und sichtbarer. Das heißt aber auch, dass wir möglicherweise stärker von Cyberkriminellen wahrgenommen werden«, sagt er. »Es ist eine Krux: Was gut ist fürs Marketing, lockt Hacker an – aber wir wissen uns ja zu schützen und zu wehren.«

Foto: MTG/Lukas Sammetinger

» Wir sind auf jeden Fall auf die NIS2 vorbereitet.«

Silvia Keitel, Geschäftsführerin MTG-Kommunikations-Technik

Weitere Informationen zur Cybersicherheit gibt es auf der IHK-Website unter: **www.ihk-muenchen.de/de/Service/Digitalisierung/Informationssicherheit/NIS-2-Kritis**

IHK-Ansprechpartner zum Thema IT-Sicherheit
Bernhard Kux, Tel. 089 5116-1705
kux@muenchen.ihk.de