
iStock

Sichere Daten

IoT-Hacking, Cyber-Erpressung, Phishing und Malware sind längst keine Fremdworte mehr im Unternehmensalltag. Cyber-Vorfälle sind mit deutlichem Abstand weltweit das Hauptrisiko für Unternehmen.

Cyber-Angriffe auf die Stadtgemeine Korneuburg, die HTL Mödling, den Batteriehersteller Varta und die österreichische Finanzmarktaufsichtsbehörde FMA sind nur ein Auszug aus der Liste der täglichen digitalen Angriffe. Laut der Studie "Cyber Security in Österreich 2023" (Link) von KPMG und Sicherheitsforum Digitale Wirtschaft stieg 2023 die Anzahl der Angriffe im Vergleich zum Vorjahr um 201 Prozent. Am häufigsten waren Phishing, Business-E-Mail-Kompromittierung, CEO-Betrug, Social Engineering und Angriffe auf die Lieferkette. Daneben sehen sich Unternehmen konfrontiert mit Deepfakes, Business E-Mail Compromise und Malware. Gefordert ist noch stärkeres Augenmerk auf die drei Schutzziele der Informationssicherheit: Integrität der Daten sowie deren Verfügbarkeit und Vertraulichkeit.

Eines der hilfestellenden Unternehmen auf diesem Weg ist Konica Minolta. Der älteste Kamerahersteller Japans bietet seit etwa zehn Jahren ein umfassendes Systemportfolio vom Endgerät über Netzwerk bis hin zu IT-Security. „Die Ära der KI wird die Attacken massiv steigern sowie komplexer machen“, vergleicht Florian Goldenstein, Chief Information Security Officer bei Konica Minolta Business Solutions Austria, die künftige Notwendigkeit von IT- und Cyber Security mit einem Vulkanausbruch. „Awareness, also die Sensibilität für das Thema, das Risiko zu erkennen und damit umzugehen, muss jedes Unternehmen haben - egal ob Einpersonen-Unternehmen oder große Enterprise-Gesellschaft“, fordert Goldenstein und beschreibt die ersten Schritte.

Zuallererst sollte man sich einen Überblick verschaffen, wo wichtige und für das Unternehmen kritische Informationen liegen, wie der Zugang ist, welche Medien genutzt

werden, ob es Backups gibt, die regelmäßig an den Sicherheitsbedarf angepasst und wie oft Daten gesichert werden. Technische Schutzmechanismen von Firewalls über Multifaktor-Authentifizierung bis hin zu automatisierten Schwachstellen-Scans sind heute in der Regel hoch entwickelt und bilden mittlerweile nicht mehr das primäre Einfalltor ins Unternehmen.

Human Firewall
Vor allem aufgrund des Fachkräftemangels und der Komplexität von IT- und Cybersecurity geht der Weg laut Sicherheitsexperten klar Richtung „Managed Service“. Noch sind laut Cyber Security Intelligence Index von IBM mehr als 90 Prozent aller Sicherheitsvorfälle auf menschliche Fehler zurückzuführen. So werden beispielsweise Links angeklickt, die zu Phishing-Seiten führen oder bösartige Webseiten aufgerufen, hinter denen Viren und andere hochentwickelte, hartnäckige Bedrohungen lauern. Daher braucht es neben klassischen Offline- und Online-Schulungen zur Informationssicherheit ein Sensibilisierungs-Training mittels realistischer Simulationen wie eine täuschend echt anmutende Phishing-Mail, ein auf dem Parkplatz liegengelassener USB-Stick oder eine fremde Person in der Video-Konferenz.

„Wir haben beispielsweise jährlich ein sogenanntes Web-based-Training, das kurze Videos zur Vermittlung der Inhalte inklusive Handlungsempfehlungen, Dokumente zum Download und Quizzes zur Selbstüberprüfung des Lernstandes umfasst. Im Verlauf des Trainings wechseln sich Phasen des Selbststudiums, Praxisphasen und Austauschphasen mehrfach ab.“

„Die digitale Landschaft entwickelt sich ständig weiter und es ist entscheidend, dass wir mit den neuesten Entwicklungen Schritt halten“, betont Florian Goldenstein. Zusätzlich unterstützt Konica Minolta Kunden mit Managed Services, beispielsweise mit

Monitoring, Patch-Management oder Backups und Endpoint-Protection. Das Wichtigste bei Sicherheitsschulungen ist laut Goldenstein, dass die Mitarbeiter*innen die Weiterbildung interessant finden, gerne daran teilnehmen und sie nicht als Pflichtveranstaltung empfinden. „Dann bleibt der Inhalt der Schulung nachhaltig im Gedächtnis." Bietet Konica Minolta das Schulungskonzept auch extern an? „Hinter den Schulungen steckt sehr viel Know-how, denn viel Erfahrung aus dem täglichen Berufsalltag ist gefragt. Der Wiedererkennungsfaktor zu eigenen Situationen muss da sein. Dafür braucht es Expert*innen. Aus diesem Grund geben wir keine Präsentationen weiter."

NIS-2
„2024 stehen wir vor einem ganz wichtigen Thema, gerade für den Mittelstand auch in Österreich", spricht Florian Goldenstein die neue EU-Richtlinie NIS-2 an, deren Ziel eine Stärkung der Cyber-Resilienz ist. Sie ist eine Weiterentwicklung der NIS-1 Richtlinie, die 2016 erlassen wurde und wichtiger Bestandteil der europäischen Cybersecurity-Strategie war. Die Schlüsselmaßnahmen der NIS-2 umfassen zehn spezifische Mindestmaßnahmen, die sogenannten TOMs (Anm. „Technische und Organisatorische Maßnahmen"), darunter Risikoanalysen, Backup-Management, Notfallwiederherstellung, Krisenmanagement, Mitarbeiterschulungen im Bereich Cybersicherheit sowie die Sicherung der Lieferkette. Bis 17. Oktober muss NIS-2 in nationales Gesetz umgesetzt sein, ab dem 18. Oktober 2024 kommt sie zur Anwendung. Die neuen Schwellenwerte sind demnach 50 Mitarbeiter*innen sowie ein Umsatz oder eine Bilanzsumme von zehn Millionen Euro. Die betroffenen Sektoren wurden auf 18 erweitert, neben der bestehenden kritischen Infrastruktur etwa auf IKT-Dienstleistungsmanagement, öffentliche Verwaltung und Forschung. In Österreich sind rund 4.000 Unternehmen betroffen. Um Unternehmen und Behörden gleichermaßen zu ermutigen, Maßnahmen zur Gewährleistung der Cybersicherheit zu ergreifen und mögliche Verstöße ernsthaft zu behandeln, drohen Bußgelder bis zu zehn Millionen Euro oder zwei Prozent des weltweiten Jahresumsatzes. „Cybersicherheit ist eine der großen Herausforderungen für uns alle. Es ist längst nicht mehr die Frage, ob ein Unternehmen angegriffen wird, sondern wann", warnt Florian Goldenstein.

Maßnahmen, die wesentlich zur Erhöhung der Cyber-Resilienz beitragen:

Technische Maßnahmen
- State-of-the-Art Firewalls, Intrusion Detection Systems und Endpoint Detection & Response Systeme
- Identifikation, Zugriffsbeschränkung mit Sensitivity Labels, Conditional Access, Multifaktor und Verschlüsselung sensibler Daten
- Regelmäßiges Backup und geübte Desaster Recovery Pläne
- Unterteilen des Netzwerks in Segmente

Organisatorische Maßnahmen
- Einrichtung eines Notfallplans
- Regelmäßige Schulungen und Sensibilisierung der MitarbeiterInnen
- Regelmäßige Prüfungen, Assessments, Penetration Test und Audits

Top Geschäftsrisiken weltweit in 2024 *(Risk Report 2024 Allianz, Link auf PDF)*
Platz 1 (36 %): Cyber-Vorfälle
Platz 2 (31 %): Betriebsunterbrechung
Platz 3 (26 %): Naturkatastrophen wie Sturm, Überschwemmung, Erdbeben

Platz 4 (19 %): Änderungen von Gesetzen und Vorschriften
Platz 5 (19 %): Makroökonomische Entwicklungen wie Inflation, Geldpolitik
Platz 6 (19 %): Feuer, Explosion
Platz 7 (18 %): Klimawandel
Platz 8 (14 %): Politische Risiken und Gewalt
Platz 9 (13 %): Marktentwicklungen wie verschärfter Wettbewerb, neue Marktteilnehmer
Platz 10 (12 %): Mangel an qualifizierten Arbeitskräften