Die Cybersecurity-Bedrohung nimmt zu – gerade für KMU

Die Anzahl an Cyberangriffen steigt und künstliche Intelligenz ermöglicht immer raffiniertere Betrugsmaschen. Expertinnen und Experten betonen daher, dass die Frage längst nicht mehr lautet, ob ein Betrieb attackiert wird – sondern wann. Der beste Schutz lautet: Bewusstsein.

Bild iStockphoto/[illegible]

1 277 Cybervorfälle in einer Woche. So viele Vorkommnisse sind laut den Zahlen des Bundesamts für Cybersicherheit (Bacs) längst Alltag geworden. Vergleicht man die Zahlen mit dem Vorjahr, wird klar, dass die Bedrohung immer grösser wird. Fachleute und Expert:innen sind längst alarmiert, sprechen von einer Zuspitzung der Lage. Zudem gelte es zu beachten, dass diese Zahlen nur die gemeldeten Vorfälle wiedergeben. Die Dunkelziffer der nicht deklarierten oder nicht erkannten Vorfälle dürfte nochmals merklich höher liegen.

Laut Marktbeobachterinnen und -beobachtern werden derzeit vor allem Malware- und Ransomware-Angriffe ausgeführt. Zudem lässt sich ein neues Phänomen beobachten: Bisher wurden Unternehmensdaten und -infrastrukturen bei Ransomware-Angriffen verschlüsselt und die Unternehmensverantwortlichen dadurch «ausgesperrt». Auf diese Weise verloren Betriebe, die über entsprechende Back-ups verfügten, zwar ihre aktuellsten Daten, doch meistens mussten nicht mehr als zwei oder drei Tage Arbeit abgeschrieben werden. Nun aber werden die Daten von den Angreifenden zusätzlich entwendet. Ist das betroffene Unternehmen nicht bereit, das geforderte Lösegeld zu bezahlen, werden die Daten im Darknet zum Kauf angeboten. Der Verlust solcher sensiblen Informationen kann gerade für KMU rasch kritisch werden.

> «
> **Umso wichtiger ist es gemäss Fachleuten, dass in KMU sowie Konzernen auf allen Betriebsebenen ein Verständnis für sicheres Verhalten kultiviert wird.**

In mehrfacher Hinsicht teuer

Nebst operationellen Unterbrüchen und Reputationsschäden können Cyberangriffe für die betroffenen Betriebe auch empfindliche Bussen nach sich ziehen. Das Schweizer Datenschutzgesetz sieht Strafen in der Höhe von bis zu 250 000 Franken für fehlbare Personen vor. Sind Daten von EU-Bürger:innen betroffen, können bis zu vier Prozent des weltweiten Umsatzes als Busse fällig werden. Problematisch ist in diesem Zusammenhang die Tatsache, dass die Angriffe immer professioneller ablaufen und sich die Chance für einen Vorfall damit erhöht. Zudem bieten moderne KI-Anwendungen zusätzliche Möglichkeiten, um sich unbefugten Zutritt zu Unternehmenssystemen zu verschaffen. Für Cyberkriminelle stellen Schweizer Unternehmen, die innovationsstark sind und hinsichtlich Cybersecurity oftmals Nachholbedarf aufweisen, daher attraktive Ziele dar.

Umso wichtiger ist es gemäss Fachleuten, dass in KMU sowie Konzernen auf allen Betriebsebenen ein Verständnis für sicheres Verhalten kultiviert wird. Hierfür können externe Partner und Bildungsinstitutionen helfen, das benötigte Fach- und Prozesswissen im Betrieb zu verankern. Spezifische Trainings und KMU-zentrierte Schulungen können wichtige Aufklärungsarbeit leisten und insbesondere auf Managementlevel aufzeigen, wie wichtig das Thema ist und welche Handlungen im Ernstfall zu priorisieren sind. Darüber hinaus empfehlen Fachleute, dass Unternehmen Notfallpläne und klare Kommunikationsstrategien entwickeln, um im Angriffsfall schnell reagieren zu können. Auch Cyberversicherungen gewinnen an Bedeutung, da sie zwar keine Prävention ersetzen, aber zumindest die finanziellen Folgen abfedern können.

Entscheidend ist jedoch nicht allein die technische Abwehr, sondern die Unternehmenskultur. Geschäftsleitungen tragen eine besondere Verantwortung, Cybersecurity als strategisches Thema ernst zu nehmen und es nicht allein der IT-Abteilung zu überlassen. Nur wenn das Bewusstsein für Risiken bei allen Mitarbeitenden geschärft wird, können Phishing-Mails erkannt, verdächtige Zugriffe gemeldet und Sicherheitslücken frühzeitig geschlossen werden. Prävention bedeutet dabei auch, regelmässig Updates einzuspielen, Passwortrichtlinien konsequent durchzusetzen und die IT-Infrastruktur systematisch auf Schwachstellen zu überprüfen. Wer diese Grundlagen vernachlässigt, riskiert im Ernstfall nicht nur hohe Kosten, sondern auch das Vertrauen von Kundinnen, Partnern und Behörden. Ein Wert, der sich nur schwer wiederherstellen lässt.

Text **SMA**