

Die Cybersecurity-Bedrohung nimmt zu – gerade für KMU

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

1 277 Cyberfälle 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.

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

Brandreport • Datarec AG

«Ohne Datenträgervernichtung bleibt Cybersecurity reines Wunschdenken»



nicht, dass hierzulande immer mehr Unternehmen Gegenmassnahmen ergreifen und ihre IT-Infrastruktur besser absichern. Doch oftmals geht dabei ein wesentlicher Faktor vergessen: «Viele Unternehmen realisieren nicht, dass auf Datenträgern essenzielle Informationen schlummern, die nicht in falsche Hände geraten sollten», erklärt Thomas Rieder, Managing Director der Datarec AG. Sein Appell ist daher klar: «Wer im Zeitalter von Social Engineering echte Cybersecurity gewährleisten will, muss den physischen Datenschutz zwingend miteinbeziehen – sonst bleibt Sicherheit reines Wunschdenken.» Genau diesen Schutz kann Datarec mit Beratung und physischer Datenvernichtung – vom PC bis zu allen Arten von Datenträgern inkl. Papier – professionell und zertifiziert gewährleisten.

Wie geht man dafür konkret vor? «Es gibt zwei Varianten», erklärt Thomas Rieder. Bei der ersten fahren die Fachleute der Datarec AG mit einem gesicherten GPS-getrackten Lastwagen beim Kundenbetrieb vor. Die Datenträger werden anschliessend in spezielle, verschliessbare Container verladen und dann innert 24 Stunden zerstört. Bei der zweiten Variante wird die Vernichtung direkt auf dem Kundenareal vorgenommen. «In beiden Fällen garantieren wir, dass man die aufgezeichneten,

gespeicherten oder gedruckten Informationen nicht wiederherstellen kann, auch nicht mit modernsten Methoden.» Zu diesem Zweck werden spezifische Schredder- und Zerkleinerungsanlagen eingesetzt, die in mehrstufigen Prozessen Papier, Festplatten, SSD-Chips, Mobiltelefone, Memorysticks und weitere Speicher aller Art ein für alle Mal vernichten und die enthaltenen Informationen nutzlos machen. Die anfallenden Rohstoffe werden anschliessend in eine nachhaltige Kreislaufwirtschaft überführt und recycelt. Datenschutz mit Nachhaltigkeit.

Sensibilisierung und Schulung der Mitarbeitenden

Die Datarec AG kommt nicht nur bei der Vernichtung von Datenträgern zum Einsatz: Die tiefgreifende Sicherheitsexpertise gibt man auch in Form von Beratungen an die Kundenfirmen weiter. «Wir nehmen die Abläufe unter die Lupe und machen unsere Kundschaft auf die verschiedenen Fallstricke aufmerksam, die Social-Engineering-Angreifende gerne als Angriffsvektor nutzen», führt Rieder aus. Als klassische Beispiele für Schwachstellen nennt er die Wahl und Hinterlegung der Passwörter, den Datentransfer auf Drittgeräte oder die Gefahr, die sich ergibt, wenn man auf sozialen Netzwerken wie

LinkedIn auch unbekannte Anfragen unkritisch annimmt. «Wir zeigen auf, welche Alltagsszenarien welches Gefahrenpotenzial aufweisen, und wie man diese Schwachpunkte gezielt ausmerzt.»

Weitere Informationen unter:
www.datarec.ch



sowie für eine unverbindliche Beratung:
+41 56 418 10 10



C yberbedrohungen nehmen in der Schweiz deutlich zu: Beim Bundesamt für Cybersicherheit (Bacs) geht im Schnitt alle 8,5 Minuten eine Meldung zu einem Cybervorfall ein. Die Dunkelziffer dürfte noch deutlich höher liegen. Angesichts dieser Häufung von Fällen überrascht es