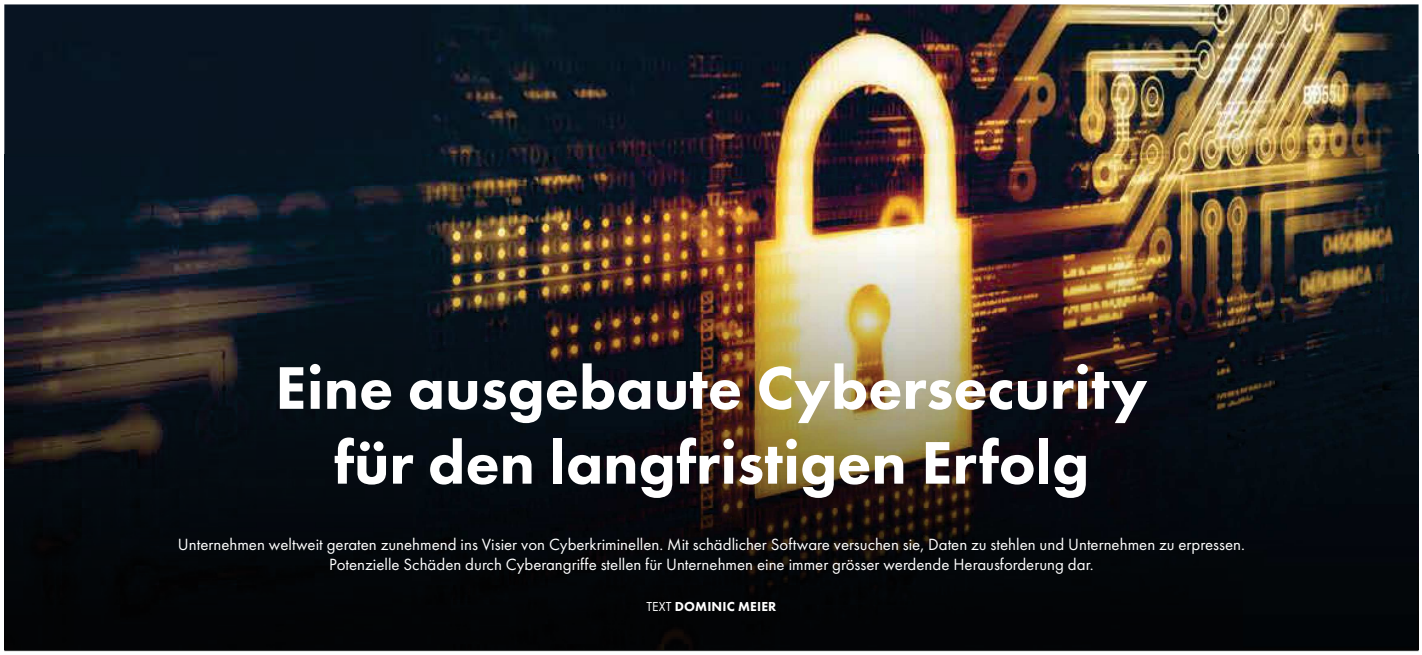

Eine ausgebaute Cybersecurity für den langfristigen Erfolg

Unternehmen weltweit geraten zunehmend ins Visier von Cyberkriminellen. Mit schädlicher Software versuchen sie, Daten zu stehlen und Unternehmen zu erpressen. Potenzielle Schäden durch Cyberangriffe stellen für Unternehmen eine immer grösser werdende Herausforderung dar.

TEXT **DOMINIC MEIER**

Unternehmen steigen vermehrt auf eine digitale Arbeitsweise um. Die rasant wachsenden Datenmengen lassen Firmen aber zur Zielscheibe von unbekannten Angreifern werden. Denn was zunächst eher Privatpersonen betroffen hat, greift immer mehr auch auf Unternehmen über: Online-Erpresser bedrohen die Cybersicherheit mit schädlicher Software und versuchen, an wertvolle Daten zu gelangen, um diese dann gegen eine Lösegeldsumme wieder einzutauschen.

Die digitale Bedrohung wächst

Für Unternehmen in der Schweiz und weltweit stellen Cybervorfälle ein hohes Geschäftsrisiko dar. Oft reicht das Budget nicht aus, um die Cybersecurity als festen Bestandteil der Unternehmensstrategie zu integrieren. Viele Unternehmen fühlen sich deshalb den Gefahren im IT-Bereich nicht gewachsen und stufen sie als grösstes Unternehmensrisiko ein. Auf der ganzen Welt sehen sich immer mehr Unternehmen mit grossen Datenskandalen und Cybererpressungen konfrontiert. Kriminelle Übergriffe auf digitaler Ebene nahmen deshalb auch zu, da Angreifer koordinierter als früher agieren und sich meist besser mit der Technik auskennen als die Betroffenen. Für Unternehmen geht die grösste Gefahr von Cybererpressungen mit Hilfe von sogenannter Ransomware aus.

Ein gefährlicher Trend

Unter Ransomware versteht man Erpressersoftwares, also Programme, die Daten verschlüsseln und unbrauchbar machen. Oftmals fordern Cyber-Kriminelle nach Aktivierung der Software von den Betroffenen eine hohe Lösegeldsumme, damit diese die Daten wieder zurückerhalten. Meist taucht dabei eine Nachricht mit der entsprechenden Forderung auf dem Desktop auf. Mit einem Countdown sorgen die Angreifer noch für zusätzlichen Druck: Wer nicht innerhalb einer gewissen Zeit zahlt, soll die Daten für immer verlieren. Der Einsatz von Ransomware ist nicht neu, sondern ein Trend, der in den letzten Jahren immer mehr zugenommen hat. Dabei tauchen auch regelmässig neue Programme auf, die mit anderen Mitteln und Funktionsweisen Firmen bedrohen. Es ist somit schwierig, sich vollumfänglich vor schädlicher Software zu schützen. Angreifer finden stets neue Wege, in Netzwerke einzudringen und an Daten zu gelangen.

Raffiniertes Vorgehen

Mit Hilfe von Viren und Trojanern versuchen Kriminelle, sich in Netzwerke von Firmen einzuschleusen. Oft geschieht dies per E-Mail, weshalb Unternehmen seit Jahren ihre Mitarbeiter entsprechend schulen. Mittlerweile haben jedoch auch gut geschulte Personen Mühe, solch potenziell gefährliche Nachrichten zu erkennen. Mit persönlich formulierten Mails sprechen Angreifer Mitarbeiter neuerdings direkt an. Auch tarnen sie die schädlichen Programme, indem sie eine Rechnung oder Bewerbung imitieren. Weiterführende Links oder Anhänge dienen hierbei als Zugang für die Ransomware. Ein einziger Klick genügt und die schädliche Software kann Daten angreifen und verschlüsseln. Teilweise haben solche Programme auch eine rein überwachende Funktion, um Logindaten der Mitarbeiter oder der Chefetage zu ergaunern und an finanzielle Daten heranzukommen. Oft sind die Angreifer Profis. Sie vernetzen sich weltweit und führen nicht nur in ihrer lokalen Umgebung Angriffe aus. Jede Branche ist betroffen, sei es Privatwirtschaft, Gesundheitswesen oder Militär. Durch die fortschreitende Digitalisierung werden Daten täglich international ausgetauscht, was den Datenberg unübersichtlich und schwer kontrollierbar gestaltet.

Lukrativ für Kriminelle, teuer für Unternehmen

Cyber-Kriminelle suchen sich ihre Opfer nicht zufällig aus. Von Ransomware betroffene Unternehmen werden gezielt aufgespürt. Je mehr Wert die Unternehmensdaten haben, desto attraktiver und anfälliger sind sie für Cyberangriffe. Bei diesen Unternehmen kann so möglichst viel mit Lösegeldforderungen herausgeholt werden. In den meisten Fällen zahlen betroffene Unternehmen die geforderte Summe, aus Angst vor einer permanenter Verschlüsselung oder einem Verlust der Daten. Ausserdem zahlen sie die Summe, um die gestohlenen Daten vor einer Veröffentlichung zu schützen. Die Schäden sind bei einem Cyberangriff weit höher als nur die bezahlte Lösegeldsumme: Ein langer Betriebsunterbruch durch befallene Server führt zu Produktion- und Umsatzverlusten, Wiederherstellungskosten und anschliessenden Liquiditätsproblemen. Der Verlust schützenswerter Daten mindert zudem das Vertrauen der Mitarbeiter und der Öffentlichkeit in die Unternehmung.

Was tun, um sich zu schützen?

Unternehmen wird empfohlen, ihre IT-Landschaft regelmässig zu pflegen und auf dem aktuellsten Stand zu halten. Technische Defekte und veraltete Schutzprogramme erleichtern Cyberkriminellen den Zugang zu betriebsinternen Daten. Zusätzlich dazu braucht es Schulungen aller Mitarbeiter im Bereich der Cybersicherheit. Die Bedrohung durch schädliche Software betrifft nicht nur die IT-Abteilung und muss als gesamtunternehmerische Herausforderung angegangen werden. Zum Schutz des Unternehmens sollten Abteilungen, die häufigen Mailverkehr betreiben und viele Anhänge öffnen, vom restlichen Netzwerk getrennt werden. Bei einem Befall durch Ransomware kann mit separaten Servern so ein Übergreifen der schädlichen Software auf andere Daten eingeschränkt werden.

Generell lohnt es sich, mehr in die Cybersecurity zu investieren. Die Digitalisierung hat in den vergangen Jahren an Fahrt gewonnen und wird auch künftig immer relevanter für Unternehmen. Ohne eine entsprechende Cybersicherheit riskieren Firmen, ihre Daten ungenügend zu schützen und dadurch anfällig für Cyberangriffe zu werden.