Cyberkriminalität: Der Mensch ist die Schwachstelle

Die einfachsten Einfalltore für Cyberkriminelle in Unternehmen bleiben Unwissenheit, Nachlässigkeit oder Neugier der Anwender. Dagegen helfen neben der Technik regelmässige Sensibilisierungen und Schulungen.

STEFAN BRÄNDLI

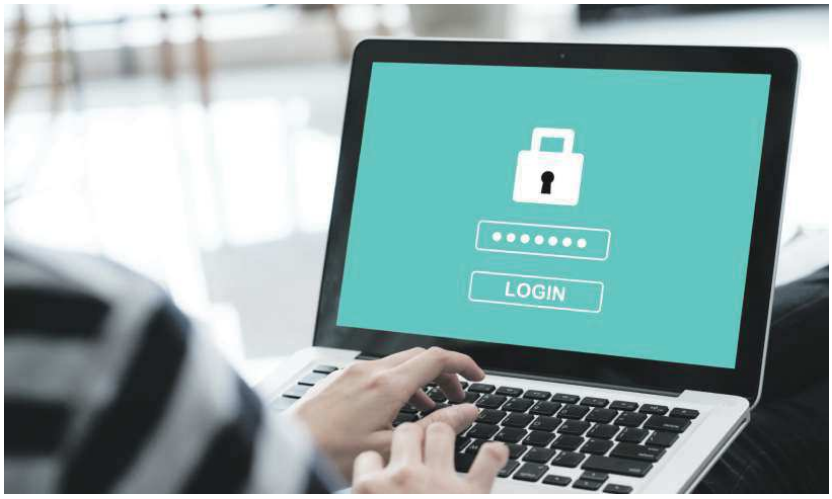
Eine aktuelle Befragung von gfs-zürich zeigt, dass KMU den Sprung ins Home-Office auf der einen Seite zwar meistern konnten, auf der anderen Seite die Cyberrisiken, die mit der Digitalisierung einhergehen, unterschätzt werden. Drei Resultate sind besonders besorgniserregend:

1. Bereits ein Viertel der Schweizer KMU waren Opfer eines folgenschweren Cyberangriffs. Knapp 13 000 Unternehmen haben einen finanziellen Schaden erlitten. Jeder zehnte Angriff führte zu einem Reputationsschaden und/oder zum Verlust von Kundendaten.

2. Nur jedes zweite KMU hat einen Notfallplan zur Sicherstellung der Geschäftsfortführung und zwei Drittel der Unternehmen haben weder regelmässige Mitarbeiterschulungen, noch haben sie ein Sicherheitskonzept.

3. Es fehlt das Bewusstsein dafür, dass das eigene Unternehmen Ziel eines Cyberangriffs sein kann. Nur 11 Prozent schätzen das Risiko, aufgrund eines Cyberangriffs einen Tag ausser Gefecht zu sein, als gross ein. Zudem sind nur knapp die Hälfte (47 Prozent) der befragten CEO über sicherheitsrelevante Themen gut informiert.

Die verstärkte Tätigkeit im Home-Office erhöht das Risiko für einen Cybervorfall. Während es am Firmenstandort relativ einfach ist, die Systeme zu überwachen und auf dem aktuellen Stand zu halten, sind viele Geräte bei den Mitarbeitern zu Hause oft ungesichert. Die Mitarbeiter benutzen den Rechner neben der Arbeit auch für private Zwecke, und es kann zumeist nicht sichergestellt werden, ob sich Schadsoftware auf dem Computer befindet. So besteht die Gefahr, dass sich Hacker Zugang zu der Betriebs-IT verschaffen – beispielsweise über «Keylogger», die Tastatureingaben eines Mitarbeiters aufgezeichnen und so die Zugangsdaten abgreifen.



Oftmals reicht eine gefälschte E-Mail-Adresse, um durch geschicktes Verhalten den Mitarbeiter zu täuschen. PD

Das eigene IT-System kennen

Um mit einem geeigneten Mitteleinsatz den besten Schutz zu erreichen, sollte man das eigene IT-System kennen und die Schwachpunkte analysieren. Zudem ist es sinnvoll, sich die wichtigsten Angriffsvektoren der Kriminellen bewusst zu werden. Kennt ein Unternehmen die eigenen Schwachpunkte, können diese punktuell angegangen werden. Investitionen in die Optimierung des Systems müssen dabei den Angriffsvektoren der Kriminellen gegenübergestellt werden. Es hilft nämlich nichts, viel Geld in ein weiteres Back-up zu investieren, um das System nach einem Ransomware-Vorfall wiederherstellen zu können, wenn keine Firewall vorhanden ist und ein Hacker schnell zum zweiten erfolgreichen Angriff ausholen kann.

Einer der häufigsten Wege, ein IT-System zu infiltrieren, ist, das System von aussen zu hacken, indem sich der Angreifer mit technischen Mitteln einen Zugang verschafft. Dies kostet jedoch Zeit und Ressourcen und lohnt sich nur, wenn entweder die IT-Security sehr tief oder das Ziel sehr lohnenswert ist.

Schwachstelle Mitarbeitende

Viel günstiger ist die zweite Methode, wenn jemand die Tür für den Angreifer öffnet. Genau darauf zielen viele Angriffsvektoren wie beispielsweise Phishing, CEO-Fraud oder Baiting ab.

Bei CEO-Fraud wird auf einen Mitarbeitenden, meist in der Buchhaltung, Druck ausgeübt, eine Zahlung auszulösen. Dabei gibt sich der Angreifer oft als CEO aus und behauptet, das Geld werde für eine Akquisition oder eine andere Anschaffung benötigt. Diese Investition sei dringend und müsse so schnell wie möglich ausgeführt werden. Das Ziel ist es, dass der Mitarbeitende die internen Kontrollmassnahmen missachtet und das Geld unter Druck schnell überweist. Bei fast allen diesen Betrugsversuchen braucht der Angreifer kein Hacker zu sein oder Zugriff auf die IT-Systeme zu haben. Es reicht eine gefälschte E-Mailadresse, um durch geschicktes Verhalten den Mitarbeiter zu täuschen. Jede Firma sollte daher die Arbeitnehmer auf solche Betrugsmaschen sensibilisieren. Dies ist die effizienteste Methode, um Schäden zu verhindern.

Stefan Brändli
ist Risk Analyst
bei Funk RiskLab

Phishing und Baiting versuchen die Unwissenheit des Personals auszunutzen. Beim Phishing werden den Mitarbeitenden E-Mails zugestellt, die einer offiziellen Adresse, z.B. von Microsoft, zum Verwechseln ähneln und dazu verleiten sollen, sich in das individuelle Microsoft-Konto einzuloggen. Die hinterlegte Eingabemaske ist aber gefälscht. Die Angreifer zeichnen die Eingabe auf, um an den Benutzernamen und das Passwort zu kommen.

Baiting (zu Deutsch «Ködern») kommt oft als vermeintlicher Gewinn daher. «Sie sind der millionste Besucher dieser Webseite und haben ein Smartphone oder Tablet gewonnen», wird dann meistens behauptet. Danach folgt die Aufforderung, persönliche Daten wie Benutzername und Passwort einzugeben. Diese Angaben gelangen direkt zu den potentiellen Angreifern. Da Internetnutzer oft den gleichen Namen und das gleiche Passwort verwenden, kommt es zum erfolgreichen Angriff.

Oftmals fehlt Sensibilisierung

Wie erwähnt werden bei zwei Dritteln der befragten Firmen keine Mitarbeiterschulungen respektive Sensibilisierungstrainings durchgeführt. Daher fehlt das Know-how, Betrugsversuche von normalen Geschäfts-E-mails zu unterscheiden. Sobald die technischen Möglichkeiten an ihre Grenzen stossen, steht nur noch die Person vor dem Bildschirm als Verteidigung zwischen den Kriminellen und dem Unternehmen.

Wichtig ist, dass die Mitarbeitenden wissen, was auf sie zukommen kann, welches die Ziele der Angreifer sind und wie reagiert werden muss, wenn man eine verdächtige E-Mail erhält. Ideal wäre es, die Mitarbeitenden über das Jahr verteilt zu einzelnen Themen zu schulen. So werden sie nicht mit einem übergrossen Ausbildungsblock überfordert und gleichzeitig auf dem aktuellen Wissensstand gehalten, da sich die Angriffstechniken auch konstant ändern.

Stefan Brändli hat sich nach seinem Masterstudium an der ETH zumeist mit Cyberrisiken beschäftigt. Als Projektleiter ist er für die Entwicklung von Funk CyberAware verantwortlich.

Leistungsstarke Cyberversicherungen bald nur noch mit Trainingsnachweis

Versicherungen prüfen Cyberrisiken immer detaillierter und stellen immer höhere Anforderungen an die Cyberfitness ihrer Kunden. Dabei erwarten sie vermehrt jährliche Mitarbeiterschulungen und Trainingsberichte zur Wahrung der Obliegenheiten eines Versicherungsvertrags. Die Versicherer offerieren Unternehmen ohne regelmässige Mitarbeiterschulungen keine oder nur sehr teure Cyberversicherungslösungen.

Ein Rundumschutz umfasst eine bedarfsgerechte technische Verteidigung (Firewall, Netzwerksegmentierung, E-Mail-Filter etc.), eine «menschliche Firewall», die regelmässig durch Schulungen auf dem neusten Stand gehalten wird, sowie eine Versicherungslösung, welche die Kosten des Schadens deckt und mit externen Spezialisten hilft, das Schadensausmass so gering wie möglich zu halten, sollten die übrigen Massnahmen versagen.

Cyberfitness für die Mitarbeitenden

Funk CyberAware deckt die wesentlichen Trainings- und Sensibilisierungsbedürfnisse ab. Die Inhalte variieren dabei nicht nur bezüglich Inhalt und Verständnisgrad, sondern auch in der Präsentation und der Didaktik. Die Trainingsprogramme stehen virtuell zur Verfügung und sind somit auch in der aktuellen Home-Office-Zeit sofort einsetzbar. Funk stellt nebst den Programmen auch die Durchführung, die Koordination und die Administration sicher. Der Wissensstand der Mitarbeitenden kann dabei getrackt und in Reports abgebildet werden. Damit lassen sich Stärken und Schwächen der Belegschaft ermitteln und danach gezielt angehen – und dies mit minimalem Aufwand seitens des Arbeitgebers.

www.funk-gruppe.ch