

Stefan Brändli

Risk Analyst Funk RiskLab
 Funk Insurance Brokers AG
 CH - 8050 Zürich
 stefan.braendli@funk-gruppe.ch
 www.funk-gruppe.ch

**Stefan Brändli**

Das schwächste Glied in jedem Cyberabwehrdispositiv ist der Mensch. Die einfachsten Einfallstore für Cyberkriminelle bleiben Unwissenheit, Nachlässigkeit oder Neugier des Anwenders. Eine aktuelle Befragung des gfs-zürich im Auftrag von digitalswitzerland, der Mobiliar, dem Nationalen Zentrum für Cybersicherheit (NCSC), der Hochschule für Wirtschaft der Fachhochschule Nordwestschweiz (FHNW) und der Schweizerischen Akademie der Technischen Wissenschaften (SATW) zeigt, dass KMUs den Sprung ins Homeoffice meistern konnten und digitaler wurden, auf der anderen Seite werden die Cyberrisiken, die mit der Digitalisierung einhergehen, unterschätzt. Dabei sind drei Resultate besonders besorgniserregend:

1. Bereits ein Viertel der Schweizer KMU waren bereits 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

DIE SCHWACHSTELLE MENSCH – CYBERKRIMINELLE NUTZEN DIESE LÜCKE GNADENLOS AUS

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

Die verstärkte Tätigkeit im Homeoffice erhöht das Risiko für einen Cyber-Vorfall noch weiter. Während es am Unternehmensstandort noch relativ einfach ist, die Systeme zu überwachen und auf dem aktuellen Stand zu halten, sind viele Geräte bei den Mitarbeitenden zuhause nicht überwacht und oft unsicher. Die Mitarbeitenden benutzen den Rechner neben der Arbeit auch noch für private Zwecke und es kann mehrheitlich nicht sichergestellt werden, ob sich Schadsoftware auf dem Computer befindet. Es besteht so die Möglichkeit, dass sich Hacker Zugang zu der Betriebs-IT verschaffen können. Zum Beispiel können über einen «Keylogger» die Tastatureingaben von Mitarbeitenden aufgezeichnet werden und so die Zugangsdaten abgegriffen werden.

Technische Möglichkeiten um die Homeoffice Tätigkeit sicherer zu gestalten sind auf dem Markt vorhanden, jedoch sind diese natürlich nicht umsonst. Es ist daher wichtig, abzuklären, mit welchem Mitteleinsatz der beste Schutz erreicht werden kann.

Dafür ist es zum einen wichtig, das eigene IT-System zu kennen und die Schwachpunkte zu analysieren. Zum anderen ist es auch sinnvoll, sich die wichtigsten Angriffsvektoren der Kriminellen bewusst zu machen. Kennt ein Unternehmen die eigenen Schwachpunkte im System, können diese punktuell angegangen werden. Die Investitionen für die Optimierung des Systems müssen den Angriffsvektoren der Kriminellen gegenübergestellt werden. Es hilft nämlich nichts, viel

Geld in ein weiteres Backup zu investieren, um nach einem Ransomware-Vorfall das System wiederherstellen zu können, wenn keine Firewall vorhanden ist und ein Angreifer schnell zum zweiten erfolgreichen Angriff ausholen kann.

Einer der wichtigsten Angriffsvektoren ist die menschliche Komponente

Die zwei häufigsten Wege ein IT-System zu infiltrieren sind erstens das System von aussen zu hacken: Der Angreifer verschafft sich mit technischen Möglichkeiten Zugang. Dies kostet jedoch Zeit und Ressourcen und lohnt sich, wenn entweder die IT-Security sehr tief oder das Ziel sehr lohnenswert ist. Nur dann ist das Kosten/Nutzen-Verhältnis für den Angreifer positiv.

Die zweite und viel günstigere Methode in ein fremdes IT-System zu gelangen ist es, wenn jemand die Tür für den Angreifer öffnet, und genau darauf zielen viele Angriffsvektoren ab: Entsprechende Techniken sind Phishing, CEO-Fraud oder Baiting.

Dies zeigt sich auch in der letzten Auswertung vom Internet Crime Complaint Center des FBI.¹ Mehr als die Hälfte des in den USA entstandenen Schadens durch Cyberkriminelle entstand durch CEO-Fraud (1.8bn\$ von 3.5bn\$).

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 sei für eine Akquisition oder eine andere Anschaffung. Diese Investition sei super dringend und müsse so schnell wie möglich durchgeführt werden. Das Ziel ist es jeweils, dass der Mitarbeitende die internen Kontrollmassnahmen nicht beachtet und das Geld unter Druck schnell überweist.

Um einen solchen Diebstahl zu verhindern ist es wichtig, dass die Belegschaft weiss, wie man sich bei Zahlungsanweisungen verhalten soll. Bei fast allen diesen

Betrugsversuchen braucht der Angreifer nicht mal ein Hacker zu sein oder Zugriff auf die IT-Systeme zu haben. Es reicht, eine gefälschte Emailadresse zu besitzen und durch geschicktes Verhalten den Mitarbeiter zu täuschen. Jedes Unternehmen sollte daher die eigenen Mitarbeitenden auf solche Betrugsmaschinen sensibilisieren. Dies ist die effizienteste Methode, um solche Schäden zu verhindern.

Bei Phishing und Baiting wird im Gegensatz zu CEO-Fraud kein Druck auf die Mitarbeitenden ausgeübt, es wird jedoch versucht, ihre Unwissenheit auszunutzen. Beim Phishing werden den Mitarbeitenden E-Mails zugestellt, die einer offiziellen E-Mail, zum Beispiel von Microsoft, zum Verwechseln ähnlich sind und Mitarbeitende dazu verleiten sollen, sich in das individuelle Microsoft-Konto einzuloggen. Die hinterlegte Eingabemaske ist jedoch gefälscht und 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 dann jedoch die Aufforderung zu persönlichen Angaben wie Benutzername und Passwort. Alle diese Angaben gelangen direkt zu den potenziellen Angreifern. Da Internetbenutzerinnen und Internetbenutzer vielfach den gleichen Namen und das gleiche Passwort verwenden, kommt es zum erfolgreichen Angriff.

Beide Angriffsmethoden funktionieren nur, weil die Mitarbeitenden nicht wissen, wie Phishing und Baiting funktionieren. Um solche Angriffe zu verhindern, ist es wichtig, die Mitarbeitenden regelmässig zu sensibilisieren und zu schulen.

Wie die eingangs erwähnte Studie jedoch zeigt, werden bei zwei Drittel der befragten Unternehmen keine Mitarbeiterschulungen respektive Sensibilisierungstrainings durchgeführt. Viele Mitarbeitende haben daher nicht das Know-how, Betrugsversuche durch Cyberkriminelle von normalen, geschäftlichen E-Mails zu unterscheiden. Sobald die technischen Möglichkeiten, gefährliche E-Mails von den Postfächern der Mitarbeitenden fernzuhalten, an ihre Grenzen stossen – und das werden sie – steht nur noch die Person vor dem Bildschirm als Verteidigung zwischen den Kriminellen und dem Unternehmen.

Wichtig ist es also, dass die Mitarbeitenden wissen, was auf sie zukommen kann, was 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. Damit werden sie nicht mit einem übergrossen Ausbildungsblock überfordert und gleichzeitig auf dem aktuellen Wissensstand gehalten, da sich die Angriffstechniken auch konstant ändern.

Leistungsstarke Cyberversicherungen bald nur noch mit Cybertrainingsnachweis

Versicherungsunternehmen prüfen Cyber Risiken 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 Versiche-

rungsvertrags. Die Versicherer offerieren Unternehmen ohne regelmässige Mitarbeiterschulungen keine oder nur sehr teure Cyber-Versicherungslösungen. Dies kann dazu führen, dass ein Unternehmen, welches keine Schulungen anbietet, auch keinen Versicherungsschutz erhält.

Empfehlenswert für einen Rundumschutz ist es, auf alle Komponenten gleich stark zu setzen: Eine bedarfsgerechte technische Verteidigung (Firewall, Netzwerksegmentierung, E-Mail-Filter, etc.), eine «menschliche Firewall» die regelmässig durch Schulungen auf dem neusten Stand gehalten wird und eine Versicherungslösung, die im Falle eines Versagens der Verteidigung die Kosten des Schadens deckt und mit externen Spezialistinnen und Spezialisten hilft, das Schadensausmass so gering wie möglich zu halten.

¹ [Source: <https://www.computerworld.ch/security/hacking/fake-chef-millionen-kostet-2617689.html>]:

Cyberfitness für Ihre 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 Homeoffice-Zeit sofort einsetzbar. Funk stellt nebst den Programmen auch die Durchführung, die Koordination und die Administration sicher. Der Wissensstand der Mitarbei-

tenden kann dabei getrackt und in Reports abgebildet werden. Damit lassen sich Stärken und Schwächen der Belegschaft ermitteln und anschliessend gezielt angehen – und dies mit minimalem Aufwand seitens des Arbeitgebers.

Hier finden Sie das Video zu Funk CyberAware:

