Social Engineering – Menschliche Schwäche als Basis für **Cyberattacken**

Unternehmen fallen dreimal häufiger Social Engineering-Attacken als tatsächlichen Schwachstellen in der IT-Sicherheitsarchitektur zum Opfer.

Warum ist das so?

Einfach ausgedrückt: Aus der Perspektive von Cyberkriminellen sind die Chancen gut und die Risiken klein. Und Cyberangriffe können mittels "Künstlicher Intelligenz" (KI) optimiert und automatisiert werden.

Frage 1:

Ist die Bedrohung durch Cybercrime / Phishing-Attacken real und relevant?

• Laut einer Cyber Security-Umfrage des TÜV sehen 92 Prozent der Befragten in Cyberangriffen eine ernstzunehmende Gefahr.

• Hornetsecurity Cyberthreat Report 2020: „Die steigende Anzahl an Cyberattacken mit zerstörerischer Malware ist besorgniserregend. Die Schäden, die Cyberkriminelle mit dieser Angriffsform verursachen können, sind immens und selbst wenn das Lösegeld für verschlüsselte Informationen nicht gezahlt wird, kann es zu langfristigen Störungen der Betriebsabläufe und damit einhergehenden großen monetären Verlusten kommen."

• Zum Vergleich: Die durchschnittliche Beute bei einem Bankraub beträgt rund 3 000 Euro; Die Durchschnittsbeute bei Business E-Mail Compromise beträgt 130 000 Euro.

• Beispiel Emotet (besonders raffinierter Wurm, zählt derzeit zu den teuersten und schädlichsten Bedrohungen weltweit): „Einmal mit Emotet infiziert, werden diese Systeme wie bei einer Wertschöpfungskette an weitere kriminelle Akteure verkauft". Es entstehen im Darknet arbeitsteilige Geschäftsmodelle „Ransomware-as-a-Service" (RaaS).

• Der finanzielle Schaden aus Erpressung mit gestohlenen oder verschlüsselten Daten betrug laut einer Umfrage des Digitalverbandes Bitkom in Deutschland in 2019 rund 10,5 Milliarden Euro!

Fazit: Ja, die Bedrohung ist real und relevant!

Frage 2:

Sind Wohnungsunternehmen gefährdet, Opfer von Phishingattacken zu werden?

• Ja, denn Wohnungsunternehmen gelten als solvent und leiden weniger unter saisonalen oder konjunkturellen Schwankungen.

• Ja, denn sie verfügen über sensible Daten von Mietern.

• Gerade kommunale Wohnungsunternehmen geraten zunehmend in den Fokus von Cyberkriminellen.

Fazit: Ja, Wohnungsunternehmen sind gefährdet.

Frage 3:

Was passiert eigentlich, wenn Angreifer sich Zugang verschafft haben?

• Wenn sich die Schadsoftware („Ransomware") erfolgreich eingenistet hat, werden die Daten verschlüsselt und nur gegen Zahlung von Lösegeld wieder entschlüsselt.

• Zunehmend drohen die Angreifer damit, vertrauliche Daten zu veröffentlichen (sogenannte Ranshameware).

• Oder es werden Daten zerstört („destructive Malware") und dabei werden auch Backup- oder Servicefunktionen beeinträchtigt.

• Die Lösegeldzahlung erfolgt über digitale Währungen wie den Bitcoin. Dies ermöglicht einen anonymen und damit für die Erpresser risikoarmen Transfer des Lösegeldes.

Frage 4:

Was muss / kann / sollte das angegriffene Unternehmen tun?

• **Aspekt Technik:** Unternehmen brauchen eine moderne und wirksame EDV-Sicherheitsarchitektur (Firewall, SPAM-Regeln etc).

• **Aspekt Technik & Organisation:** Plan- und regelmäßige Datensicherungen, zeitnahe Updates von allen verwendeten Programmen, Systemen und Anwendungen. Die jüngsten Erfahrungen im Bereich Microsoft Exchange Mail-Server haben verdeutlicht, dass in diesem Bereich große Risiken entstehen können (Patches wurden nicht eingespielt) und zu lange bestehen bleiben (z.B. 5. März 2021 „BSI warnt: Kritische Schwachstellen in Exchange-Servern – Sofortiges Handeln notwendig!")

• **Aspekt Organisation:** Jeder einzelne Mitarbeitende muss die ihn betreffenden Risiken kennen und sich der Risiken bewusst sein. Er muss potenzielle Bedrohungen erkennen und wissen, was zu tun und was zu lassen ist. Schulungen können helfen, Wissen und Verständnis aufzubauen. Unserer Erfahrung nach braucht es dazu Schulungskonzepte, die arbeitsplatz- und arbeitsalltagstauglich sind, Stichwort: Lernen am Arbeitsplatz/video-basiertes E-Learning. Praktische Übungen durch sogenannte Phishing-Übungen helfen das Wissen ins Bewusstsein zu bringen. Denn die Erkenntnis und die Erfahrung, dass ein soeben getätigter Klick auf einen Link – wäre es nicht eine Übung gewesen – massiven Schaden hätte anrichten können, löst nachhaltige Lernerfahrungen in der betroffenen Person aus.

Fazit: Das Zusammenspiel aus EDV-Sicherheitsarchitektur, organisatorischen Routinen und die Schulung der Belegschaft bietet den besten Schutz. Eine Phishing-Übung simuliert eine Cyber-Attacke und macht damit sichtbar, wie gut das Risikobewusstsein wirklich ausgeprägt ist und die Belegschaft ihren Teil im Sicherheitskonzept zu leisten imstande ist. Der vdw bietet seinen Mitgliedsunternehmen sowohl eine Schulungsplattform **https://vdw-online.trainstitute.de/** als auch Phishing-Übungen in Kooperation mit der Firma Trainstitute® an. Sollten Sie Interesse an der Durchführung einer Übung haben, füllen Sie bitte die Bedarfsabfrage **https://trainstitute.de/bedarfsabfrage/** aus. ←