ERFOLGREICHE IT-SICHERHEIT GEHT ALLE AN

Egal welche Informationssicherheitsstudie gelesen wird, immer wird der Mensch als schwächstes Glied der Schutzkette bezeichnet. Je nach Studie sind bis zu 90 % der Vorfälle die eigenen Mitarbeitenden. Oft steckt gar keine Absicht dahinter, sondern Unwissenheit oder einfach nur Bequemlichkeit. Eine regelmässige Awareness hilft, mögliche erfolgreiche Angriffe zu reduzieren.

Von Andreas Wisler

Während heutige Technik nur zwischen Schwarz und Weiss entscheiden kann, erkennt der Mensch auch die Zwischenfarben. Antiviren-, Antispam- und Firewallsysteme versuchen anhand von Mustern oder Abweichungen zu erkennen, ob es sich um einen Angriff handelt oder nicht. Doch die Hacker auf der anderen Seite schlafen nicht und versuchen immer wieder über neue Wege durch die Barrieren zu gelangen. So gelangen E-Mails und Webseiten durch die Filter bei den Mitarbeitenden. Diese müssen nun entscheiden, klicke ich oder klicke ich nicht.

Viele Angriffe werden mittels E-Mail durchgeführt. Mit so genannten Phishing-E-Mails wird versucht, die Person in Sicherheit zu wiegen und sie zu verleiten, auf den Link oder das Attachment zu klicken. Entweder der Virus versteckt sich bereits in der E-Mail oder in der aufzurufenden Webseite. Auch kann es sein, dass der Link zu einer Seite führt, wo ein Login abgefragt wird. Unbedarft werden dann die Zugangsdaten eingegeben, sieht ja so aus, wie bei uns in der Firma oder bei Facebook, und schon sind persönliche Daten in fremden Händen.

Awareness-Massnahmen helfen, die Angriffsfläche zu reduzieren. Doch dies ist gar keine einfache Aufgabe. Laut einer NIST-Studie von Oktober 2016 sind 63 % der befragten Personen Security-Müde. Als Gründe dafür werden zu viele Informationen, falsches Niveau, zu wenig konkrete Handlungsanweisungen oder Hilflosigkeit genannt.

Dies zeigt, wie diffizil eine erfolgreiche Awareness-Kampagne ist. Wie können nun IT-Sicherheitsbeauftragte reagieren? Nichts tun? Regelmässig E-Mails ver-

schicken? Angst oder Vorwürfe machen? Oder alle zwei Jahre eine Schulung durchführen? Vermutlich wird nichts davon zum Ziel führen, die Informationssicherheit nachhaltig zu erhöhen.

Wichtig ist, die verschiedenen Menschen und Lerntypen (nach Vester) zu motivieren, so dass die visuellen, auditiven, kognitiven und haptischen Sinne angesprochen werden. Folgende Möglichkeiten stehen dabei als Möglichkeiten zur Verfügung:

- **Social Engineering-Angriffe**
  Per Phishing-E-Mails, Telefon oder persönlich vor Ort wird versucht, an Informationen zu kommen. Selber das Gefühl zu spüren, «Mist, ich bin reingefallen», hilft auch gut gefälschte E-Mails in Zukunft zu erkennen. Wichtig ist aber, nie den Menschen persönlich bloss zu stellen. Daher sollte die Auswertung anonym erfolgen. Wissenschaftliche Studien zeigen, dass ein persönlicher Angriff die Psyche eines Menschen negativ beeinflussen kann.

- **Präsentationen**
  Der interne Spezialist hat es hier oft schwer. Fremden Propheten wird viel eher vertraut. Gut geschulte Referenten können die Mitarbeitenden auf allen Ebenen ansprechen. Live Demos zeigen, wie Hacker vorgehen, welche Tools sie einsetzen und die Wirkung bleibt oft lange im Hinterkopf bestehen.

- **E-Mails**
  E-Mails sollten mit Bedacht eingesetzt werden. Die Mitarbeitenden versinken heute in einer Flut von E-Mails, da werden solche «unwichtigen» Nachrichten gerne auf später verschoben. Bei wichtigen und akuten Ereignissen ist es jedoch die schnellste Möglichkeit, alle zu informieren.

- **Videos**
  Der Mensch reagiert viel intensiver auf bewegte Bilder. Die Videos können bestimmte Situationen eindrücklich zeigen. Gut gemachte Videos helfen, Wissen effektiv zu vermitteln. Aber auch hier sollten nicht zu viele Videos auf einmal gezeigt werden.

- **E-Learning**
  Der Vorteil von E-Learning-Plattformen ist, dass sich alle Mitarbeitenden dann weiterbilden können, wenn sie Zeit dafür haben. E-Learning-Plattformen sind oft eine Kombination aus Texten, Situationen, Videos und Audio-Dateien. Gleichzeitig kann eine Lernkontrolle anhand Tests erfolgen.

- **Gadgets**
  Wer hat nicht gerne ein «Spielzeug»? Security-Gadgets erinnern immer wieder an das Gelernte.

- **Plakate**
  Auch Plakate sind eine gute Möglichkeit, auf bestimmte Punkte aufmerksam zu machen. Zum Beispiel, wie sichere Passwörter erstellt werden oder wie die internen Weisungen aussehen. Auch hier gilt, zurückhaltend verwenden.

Ein Werkzeug alleine kann die Informationssicherheit bereits erhöhen. Doch dies klingt schnell wieder ab. Der Alltagsstress lässt das Gelernte wieder in Vergessenheit geraten. Regelmässige Awareness bringt oft mehr, als eine einzelne Schulung. Getreu dem Motto «steter Tropfen höhlt den Stein», sollten in geplanten Abständen verschiedene Aktionen durchgeführt werden. Die Mitarbeitenden sollen spüren, dass sie eine wichtige Rolle in der Informationssicherheit haben. Wenn alle am gleichen Strick – und vor allem auf der gleichen Seite – ziehen, kann die Angriffsfläche für erfolgreiche Angriffe massiv reduziert werden.

WEITERE INFORMATIONEN

www.goAware.ch

Andreas Wisler
Inhaber und Senior Security Auditor
der goSecurity GmbH
www.goSecurity.ch

Link zur Studie:
nist.gov/news-events/news/2016/10/security-fatigue-can-cause-computer-users-feel-hopeless-and-act-recklessly