Im Visier der Hacker

Jakob Schmidt

Erfolgversprechende Cybersecurity-Strategien beruhen auf drei Säulen: Mensch, Technologie sowie Organisation und Prozesse. Allerdings wird die zentrale Säule – der Mensch – allzu oft sträflich vernachlässigt.

Um die mannigfaltigen Gefahren abzuwehren, die der IT-Infrastruktur aus den Tiefen des Internets drohen, wird kräftig in hochmoderne Security-Systeme investiert. Doch: Je besser Technik Gefahren von außen erkennt und abwehrt, umso attraktiver wird es, diese zu umgehen und die Menschen, die schon Zugang zu den Systemen haben, zu hacken. Um es mit dem amerikanischen Security-Experten Bruce Schneier zu sagen: „Nur Amateure greifen die Technologie an, Profis nehmen den Menschen ins Visier." Dabei ziehen sie alle Register des Social Engineering und nutzen Grundverhaltensmuster des Menschen aus. Sie appellieren an seine Hilfsbereitschaft, arbeiten mit (Zeit-)Druck, schüren Ängste oder versprechen befristete Belohnungen.

Die drei Säulen einer Cybersecurity-Strategie.

Manchmal kommen die Angriffe plump daher, etwa in Form von skurril anmutenden Anrufen oder Massen-Spammails, die, wenn man weiß, worauf man achten soll, ohne Weiteres als solche zu erkennen sind. Aber immer öfter sind Angriffe sehr viel zielgerichteter. In der Vorbereitung sammeln Cyber-Kriminelle alle Daten, an die sie herankommen können: über das Telefon, vor Ort getarnt als Servicemitarbeiter, in den sozialen Medien und dem Web. Diese Daten werden verknüpft, verarbeitet, ausgewertet und dienen als Grundlage eines ausgeklügelten Angriffsplans. Nicht selten ist dieser sogar mehrstufig aufgebaut. Etwa in Schritt 1 den Zugriff auf das Mail-Postfach eines Mitarbeiters in Behörde A zu bekommen, um dann in Schritt 2 als vermeintlich vertrauenswürdige Person einen Mitarbeiter bei Behörde B ins Visier zu nehmen.

Ein Evergreen ist das Versenden einer Bewerbung, die im Hintergrund (meist über die Makrofunktionalität) unerwünschte Schad-Software mit sich bringt. Ein kurzer Anruf des vermeintlichen Bewerbers, mit der Bitte, einmal schnell nachzuschauen, ob der aktuelle Lebenslauf dabei sei, die Versicherung, das mit den Makros sei schon okay, und der Schaden ist geschehen. Fakt ist, Cyber-Kriminelle haben mittlerweile einen hohen Grad an Professionalität erreicht. Da ist es fahrlässig, seine Mitarbeiter auf Amateurniveau zu belassen.

Cyber-Security beruht auf drei Säulen: Mensch, Technologie sowie Organisation und Prozesse. In der Realität wird aber meistens die Technologie implementiert, passende Prozesse erarbeitet und dann den Mitarbeitern übergestülpt. Das führt zu Problemen, schließlich wird damit in jahrelang erprobte Abläufe des Arbeitsalltags einge-

griffen. Die Folge: Widerstand. Viele Mitarbeiter versuchen alles, die praktizierten Vorgehensweisen weiterhin zu nutzen. Notfalls unter Umgehung der neuen Regeln. Das Problem liegt aber nicht nur beim Mitarbeiter, sondern daran, dass er bei der Erarbeitung des Konzepts nicht im Mittelpunkt stand. Sonst hätte man sich Gedanken darüber gemacht, inwiefern sein Arbeitsalltag betroffen ist, und bei gravierenden Änderungen deren Notwendigkeit erklärt.

Fehlende Erklärungen, mangelhafte Kommunikation, vernachlässigte Orientierung am Arbeitsalltag und schwach ausgebildetes Awareness-Bewusstsein – das sind die Zutaten, die ein auf dem Papier genial anmutendes Cybersecurity-Konzept in der Realität krachend scheitern lassen. Ebenso in den Bereich der Kommunikation gehört das Thema Ansprechpartner: An wen wenden sich die Mitarbeiter bei Verdachts- oder Schadensfällen? Allzu oft ist das nicht wirklich bekannt, muss in einer Notsituation erst einmal nach dem Ansprechpartner recherchiert werden.

Angriffsfläche für Cyber-Kriminalität bietet auch die hierzulande übliche Devise: Fehler kommen im Job nicht vor. Wer dennoch welche macht, steht am Pranger. Das führt zu einer Angstkultur, in der Fehler vertuscht und verschleppt werden. Im Fall eines Cybersecurity-Vorfalls ist dieses Verhaltensmuster ein Super-GAU, da Zeit ein entscheidender Faktor bei der Eindämmung ist. Dieses Phänomen betrifft zwar die Mitarbeiter, seine Ursache liegt aber in der Unternehmenskultur. Solange kein anderer Umgang mit Fehlern gelebt wird, ist das Problem kaum in den Griff zu bekommen. Aus Security-Sicht ist eine Kultur nötig, die das Vorkommen von Fehlern akzeptiert, diese schnell und offen kommuniziert und daraus die richtigen Lehren zieht. Ein zusätzlicher Vorteil einer solchen Unternehmenskultur: Die Mitarbeiter trauen sich mehr zu, agieren selbstständiger und kreativer und gleichzeitig aufmerksamer, wenn sie wissen, dass ihnen aus einem Fehler kein Strick gedreht wird.

Im Rahmen einer Zertifizierung oder Rezertifizierung, beispielsweise auf Grundlage der ISO 2700x-Reihe, reicht es zwar aus, den Nachweis zu erbringen, dass die Mitarbeiter geschult wurden. Meistens passiert das aber als fast schon einschläfernder Frontalunterricht unter Zuhilfenahme überfrachteter Power-Point-Präsentationen. Nachweis erbracht – Ziel erreicht? Nicht wirklich! Das Ziel der Übung sollte ja eigentlich sein, die Mitarbeiter für das Thema Cyber-Risiken zu sensibilisieren, und nicht, ein Häkchen im Rahmen der Zertifizierung zu bekommen. Besser als einmalige Veranstaltungen ist es, das Thema Awareness in den Arbeitsalltag einzubauen.

Ebenso, wie Hacker sich beim Social Engineering die menschliche Psyche zunutze machen, kann man das auch auf der Gegenseite. Der Drang nach Lob ist tief im Menschen angelegt und lässt sich einfach ansprechen durch kleine virtuelle Belohnungen in Form von Trophäen, Badges und ähnlichem. Der Mensch muss mit der Technologie umgehen, die Prozesse in der täglichen Arbeit anwenden und leben. Daher ist es sinnvoll, Cybersecurity von ihm aus zu denken. Ohne das aktive Mitwirken durch den Menschen ist nämlich jede Cybersecurity-Strategie von Beginn an zum Scheitern verurteilt. Daher ist es höchst sinnvoll, dem Thema Awareness einen entsprechenden Stellenwert einzuräumen.

Jakob Schmidt ist Coordinator Awareness KORAMIS im Kompetenzzentrum für Cybersecurity der telent GmbH.