Cybersecurity

Bewusstsein schaffen

Immer öfter greifen Hacker IT-Systeme von Behörden und kommunalen Einrichtungen an. Ein wichtiger Schritt, um das zu vermeiden, ist eine gute Schulung des Personals, um es für die drohenden Gefahren zu sensibilisieren.

Ein erfolgversprechender Cybersecurity-Ansatz ist ganzheitlich und richtet den Blick auf die drei tragenden Säulen: den Menschen, die Technologie und die Organisation. In der Realität sieht die Sache oft anders aus. Wird investiert, um die IT-Infrastruktur gegen Gefahren aus dem Internet zu schützen, dann meist in Technik und die Erarbeitung und Umsetzung zeitgemäßer Prozesse. Ausgerechnet beim zentralen Faktor Mensch schlägt der „Sparhans“ zu. Plötzlich ist kein Budget mehr vorhanden an einer Stelle, an der die Investitionen im Vergleich gering sind, aber unmittelbar das Cybersecurity-Level verbessern. Das rächt sich im Fall der Fälle. Da die Security-Technik immer besser Gefahren von außen erkennt und abwehrt, wird zunehmend der Mensch zum Einfallstor. Dafür ziehen Cyberkriminelle alle Register des Social Engineering und nutzen tief im Menschen angelegte Verhaltensmuster, indem sie etwa an die Hilfsbereitschaft appellieren, (Zeit-)Druck aufbauen oder Ängste schüren.

Cyberkriminelle haben einen hohen Grad an Professionalität erreicht. Da ist es fahrlässig, Mitarbeiter auf Amateurniveau zu belassen. Angriffe wie Massenspams sind noch einfach zu erkennen, wenn man weiß, worauf man achten soll. Doch immer öfter sind Angriffe sehr viel ausgeklügelter. In der Vorbereitung sammeln Cyberkriminelle alle Daten, an die sie herankommen können: über das Telefon, soziale Medien, das Web oder vor Ort getarnt als Servicemitarbeiter. Die Daten werden verknüpft, verarbeitet, ausgewertet und dienen als Grundlage eines zielgerichteten, häufig mehrstufigen Angriffsplans. Etwa, um in Schritt eins den Zugriff auf das Mailpostfach eines Mitarbeitenden in Behörde A zu bekommen, um dann in Schritt zwei als vermeintlich bekannte und vertrauenswürdige Person einen Mitarbeitenden bei Behörde B zu kontaktieren. Ein Bewusstsein für diese Gefahren bei der Belegschaft zu schaffen und hoch zu halten, ist eine der mächtigsten Waffen im Kampf gegen Cyberkriminalität.

Foto: Adobe Stock/contrastwerkstatt

Da die Sicherheitstechnik immer besser Gefahren von außen erkennt und abwehrt, wird zunehmend der Mensch zum Einfallstor für Hackerangriffe.

Angriffsfläche bietet auch die Devise: Fehler kommen im Job nicht vor. Das geht einher mit 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 den Faktor Mensch, 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 braucht es eine Kultur, die Fehler akzeptiert, sie schnell und offen kommuniziert und die richtigen Lehren zieht.

FOKUS NICHT NUR AUF TECHNIK

Die drei Grundpfeiler der Cybersecurity werden in der Praxis selten gleichberechtigt bedacht, sondern meist mit dem Schwerpunkt auf der Technik. Eine technische Lösung wird implementiert, passende Prozesse erarbeitet und dann den Mitarbeitenden übergestülpt. Das führt zu Problemen – es wird in jahrelang erprobte Abläufe des Arbeitsalltags eingegriffen. Die Folge: Widerstand, um die praktizierten Vorgehensweisen beizubehalten; notfalls unter Umgehung der neuen Regeln. Das Problem liegt nicht nur beim Personal. Sondern darin, dass es bei der Erarbeitung des Konzepts nicht im Mittelpunkt stand.

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 scheitern lassen. In den Bereich der schlechten Kommunikation gehören auch Mitarbeiterschulungen, die häufig als fast schon einschläfernder Frontalunterricht stattfinden. Besser als einmalige Veranstaltungen ist es, das Thema Awareness in den Arbeitsalltag einzubauen. Kurze, dafür regelmäßige Einheiten halten das Thema präsent und rufen es im Gedächtnis immer wieder nach vorne.

Ebenso, wie Hacker sich beim Social Engineering die menschliche Psyche zunutze machen, kann man das auf der Gegenseite. Der Drang nach Lob ist tief im Menschen angelegt und lässt sich einfach durch kleine virtuelle Belohnungen, wie Trophäen oder Badges, ansprechen.

Der Mensch muss Cybersecurity in der täglichen Arbeit leben. Ohne sein Mitwirken scheitert jedes noch so gute Konzept. Daher ist es sinnvoll, dem Thema Awareness einen hohen Stellenwert einzuräumen und bei der Umsetzung alle Möglichkeiten in Betracht zu ziehen, anstatt immer wieder die gleichen ausgelatschten Pfade zu betreten.

Jakob Schmidt

DER AUTOR

Jakob Schmidt ist Coordinator Awareness KORAMIS, Kompetenzzentrum für Cybersecurity der telent GmbH, Backnang