Foto: Telent

Nimmt eine Cybersecurity-Strategie die Mitarbeiter nicht mit, muss sie scheitern. Ein wirksamer Ansatz muss immer ganzheitlich sein.

Anwenderprobleme lösen

Fünf hausgemachte Probleme, die jedes Cybersecurity-Konzept aushebeln – und wie man diese ganzheitlich löst.

JAKOB SCHMIDT

Ein erfolgversprechender Cybersecurity-Ansatz ist ganzheitlich und beruht auf den drei Säulen Mensch, Technologie sowie Organisation und Prozesse. Trotzdem wird die zentrale Säule Mensch oft sträflich vernachlässigt – mit fatalen Folgen. Denn nimmt eine Cybersecurity-Strategie die Mitarbeiter nicht mit, muss sie scheitern. Um IT-Infrastruktur gegen die Gefahren aus dem Internet zu schützen, wird kräftig investiert: in hochmoderne Technik, die Erarbeitung und Umsetzung zeitgemäßer Prozesse und – falls notwendig – wird sogar die gesamte Security-Organisation umgekrempelt.

Problem 1: An der falschen Stelle gespart

Ausgerechnet beim zentralen Faktor Mensch schlägt der „Sparhans“ zu. Plötzlich ist kein Budget mehr vorhanden an einer Stelle, an der die Investitionen geradezu lächerlich gering sind, aber unmittelbar das Cybersecurity-Level verbessern. Das rächt sich im Fall der Fälle. Mehr als 50 Prozent der im Rahmen der IDG Studie Cybersecurity 2020 befragten Unternehmen ist bereits ein finanzieller Schaden durch Cyberattacken entstanden. Provokativ gesagt: Ein einziger Tag Produktionsausfall ist um ein zigfaches teurer als ein paar Euro für Awareness-Maßnahmen.

> „Jede Cybersecurity-Strategie ist nur so gut, wie ihr schwächstes Glied. “
>
> **Jakob Schmidt,** telent GmbH

Problem 2: Cyberkriminelle nehmen Mitarbeiter gezielt ins Visier

Da die Security-Technik immer besser Gefahren von außen erkennt und abwehrt, wird zunehmend der Mensch wichtiger. Dafür ziehen Cyberkriminelle alle Register des Social Engineering und nutzen Verhaltensmuster aus, indem sie an die Hilfsbereitschaft appellieren, (Zeit-)Druck aufbauen oder Ängste schüren.

Angriffe, wie Massenspams, sind einfach zu erkennen, wenn man weiß, worauf man achten soll. Immer öfter sind Angriffe sehr viel ausgeklügelter. Zur Vorbereitung sammeln Cyberkriminelle Daten

per Telefon, sozialen Medien und Web. Diese werden verknüpft und ausgewertet, um darauf einen oft mehrstufigen Angriffsplan aufzubauen. Geht es im ersten Schritt darum, Zugriff auf das Mailpostfach eines Mitarbeiters der Firma A zu bekommen, kann darüber als vermeintlich bekannte Person im nächsten Schritt ein Mitarbeiter bei Firma B ins Visier genommen werden. Ein Evergreen ist das Versenden einer Bewerbung, die meist über die Makrofunktionalität unerwünschte Schadsoftware mit sich bringt. Bittet der vermeintliche Bewerber dann telefonisch, nachzuschauen, ob der aktuelle Lebenslauf dabei sei, ist der Schaden schnell geschehen. Fakt ist, Cyberkriminelle werden immer professioneller. Da ist es fahrlässig, Mitarbeiter auf Amateurniveau zu belassen.

Problem 3: Primat der Technologie

Cybersecurity beruht auf drei Säulen. Doch tatsächlich wird meist nur die technische bedacht, indem Technologien implementiert, passende Prozesse erarbeitet und dann der Belegschaft übergestülpt werden. Die Folge: Widerstand. Viele Mitarbeiter werden alles versuchen, jahrelang praktizierte Vorgehensweisen weiterhin beizubehalten. Das Problem entsteht vor allem, wenn sich niemand bei der Konzepterarbeitung Gedanken über veränderte Arbeitsabläufe macht und deren Notwendigkeit erklärt.

Mangelhafte Kommunikation, vernachlässigte Orientierung im Arbeitsalltag und schwach ausgebildete Awareness – 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. Allzu oft ist nicht bekannt, an wen sich Mitarbeiter im Verdachts- oder Schadensfall wenden sollen und müssen das erst recherchieren.

Problem 4: Wenn die vermeintliche Perfektion zum Verhängnis wird

Hätte es Rückfragen zur vermeintlichen CEO-Mail gegeben, wäre der Betrug wahrscheinlich aufgeflogen. Dass dies nicht erfolgte, liegt auch an einer hierzulande typischen Verhaltensweise, die auf einer weitverbreiteten, fragwürdigen Unternehmenskultur beruht: Wer Fehler macht, steht – zumindest gefühlt – am Pranger. Deswegen werden sie lieber vertuscht oder verschleppt. Im Fall eines Cybersecurity-Vorfalls ist das ein Super-GAU, da Zeit ein entscheidender Faktor bei der Eindämmung ist. Nicht nur aus Security-Sicht ist eine Unternehmenskultur geboten, die akzeptiert, dass Fehler vorkommen und diese schnell und offen kommuniziert, um aus ihnen die richtigen Lehren zu ziehen. Ein zusätzliches Bonbon einer solchen Kultur: Mitarbeiter trauen sich mehr zu, agieren selbständiger, kreativer und gleichzeitig aufmerksamer, wenn sie wissen, dass ihnen aus einem Fehler kein Strick gedreht wird.

„Cyberkriminelle ziehen alle Register des Social Engineering und nutzen Verhaltensmuster aus, indem sie an die Hilfsbereitschaft appellieren, (Zeit-)Druck aufbauen oder Ängste schüren."

Problem 5: Gähnende Langeweile

Keine Frage, im Rahmen einer Zertifizierung oder Rezertifizierung beispielsweise auf Grundlage der ISO 2700x-Reihe reicht der Nachweis der Mitarbeiterschulung. Meistens passiert das in einschläferndem Frontalunterricht unter Zuhilfenahme überfrachteter Power-Point-Präsentation. Nachweis erbracht – Ziel erreicht? Nicht wirklich! Das Ziel der Übung sollte ja eigentlich sein, die Mitarbeiter für das Thema Cyberrisiken zu sensibilisieren. Awareness auf Seiten der Mitarbeiter ist eine der mächtigsten Waffen im Kampf gegen die zahlreichen Gefahren, die der eigenen IT-Infrastruktur drohen. Besser als eine einmalige Veranstaltung ist es, das Thema in den Arbeitsalltag einzubauen mit kleinen, dafür regelmäßigen Bausteinen.

So wie Hacker sich beim Social Engineering die menschliche Psyche zu Nutze machen, können das auch Unternehmen. Der Wunsch nach Lob ist tief im Menschen angelegt. Warum ihn nicht in Form von virtuellen Belohnungen, wie Trophäen oder Badges, befriedigen. Weil Arbeit kein Computerspiel ist? Stimmt. Aber trotzdem spricht so etwas das Belohnungszentrum an.

Da der Mensch die Technologie und Prozesse aktiv in seiner täglichen Arbeit leben muss, ist Cybersecurity von ihm aus zu denken. Denn jede Cybersecurity-Strategie ist nur so gut, wie ihr schwächstes Glied. Daher ist es höchst sinnvoll, der Awareness einen entsprechenden Stellenwert einzuräumen, statt immer wieder die gleichen, mit Verlaub etwas ausgelatschten Pfade zu betreten. ■

telent GmbH:
www.telent.de