Wenn Stress zum Sicherheitsrisiko wird

Mitarbeitende müssen heute nicht nur die steigende Informationsflut bewältigen, sondern auch ständig vor betrügerischen Mails auf der Hut sein. Statt Informationssicherheit als konstante Bedrohung zu thematisieren, sollten Unternehmen versuchen, ihre Mitarbeitenden zu entlasten.

«Der Mensch ist die Schwachstelle Nummer eins.» Diesen Satz hören viele Angestellte im heutigen Arbeitsumfeld immer häufiger. Schlagzeilen gibt es zuhauf: Datenlücken, Lösegeldforderungen, Stillstände in Fabriken. «Schuld» sind oftmals Angestellte, die im E-Mail-Posteingang einen falschen Link öffnen oder auf die falsche Mail antworten.

Die Rede ist dabei von Social Engineering. Der Ausdruck bezeichnet eine Methode für Cyberkriminelle, über Angestellte eines Unternehmens Zugang zu vertraulichen Informationen zu erhalten – meist über Phishing-E-Mails. Social Engineering gehört heute zu den grössten Bedrohungen für Unternehmen. So investieren diese in Cybersecurity-Trainings für die Belegschaft, stellen zig Verhaltensregeln auf oder versenden sogar fingierte Phishing-Mails, um «Awareness» zu schaffen und ihre Angestellten auf die Probe zu stellen.

Der Posteingang als Stressfaktor

Trotzdem hat die Erfolgsrate von Phishing- und Spear-Phishing-Attacken über die letzten Jahre zugenommen. Die Vermittlung von Grundlagen zur Erkennung bösartiger E-Mails ist eine Sache, aber noch wichtiger ist es, genau zu verstehen, was die Mitarbeitenden dazu bewegt, auf die Links von Phishing- und Betrugs-E-Mails zu klicken. Gemäss diversen Studien existieren verschiedene begünstigende Attribute, etwa das Geschlecht oder das Alter. Doch es gibt auch andere Faktoren wie Unkonzentriertheit, Erschöpfung und Stress.

Das E-Mail-Postfach ist Dreh- und Angelpunkt im Arbeitsalltag vieler Angestellter. Jährlich steigt das Volumen versendeter und empfangener Mails, besonders seit Beginn der Pandemie. Dementsprechend fordernd, gar stressig ist der tägliche Umgang mit dem E-Mail-Postfach. Studien belegen, dass ein hohes E-Mail-Volumen die psychische Belastung und die Entwicklung negativer Emotionen erhöht. Darüber hinaus wirkt sie sich auf die Leistung der Mitarbeitenden bei arbeitsbezogenen Aufgaben aus, wodurch das Stresslevel weiter steigt.

Bild: ©fizkes - stock.adobe.com

Druck durch Cyberbedrohungen

Hinzu kommt der psychische Druck, den Angestellte aufgrund steigender Cyberbedrohungen erleben. Sie sehen sich als «latente Gefahr», als Einfallstor für Cyberkriminelle. Die Pandemie zwang sie, von zuhause aus zu arbeiten, wahrscheinlich in einer nicht so sicheren Netzwerkumgebung wie im Büro – was den Druck, die richtigen Entscheidungen zu treffen, weiter erhöhte. Nicht zuletzt erfahren Angestellte Druck durch Schlagzeilen in den Nachrichten sowie im Rahmen firmeninterner Memos oder Awareness Trainings. Dieser mentale Stress führt nicht nur zu einer ungesunden Arbeitskultur, er verleitet auch vermehrt zu Fehlern. Fehler, die das ganze «Awareness-Training» in Sekundenschnelle zunichtemachen können. Mit nur einem Klick.

Entlastung der Mitarbeitenden als Sicherheitsmassnahme

Die Frage drängt sich auf, ob und wie Unternehmen ihre Cybersecurity-Strategie überdenken sollten – mit dem Ziel, sich mit den tatsächlichen, zugrunde liegenden Faktoren zu befassen, die Schwachstellen verursachen. Es ist die Aufgabe der Unternehmen sowie der Unternehmensführung, die richtigen Bedingungen für ihre Mitarbeitenden zu schaffen. Das bedeutet, Lösungen zu finden, die die Sicherheit der Mitarbeitenden und der Unternehmensassets erhöht, ohne dabei den Stress des Einzelnen zu steigern.

Der Autor
Philipp Bachmann, COO und Sales/Channel Manager, SEPPmail
bachmann@seppmail.ch

Das Dossier finden Sie auch online
www.swisscybersecurity.net