In so genannten Awareness-Schulungen werden unter anderem Tricks von Cyber-Kriminellen aufgezeigt.

FOTO: SHUTTERSTOCK

Unsicherheitsfaktor Mensch

Awareness-Schulung sensibilisiert für Risiken

Beim Thema IT-Sicherheit haben die meisten Unternehmen in erster Linie die technische Ausstattung wie Firewalls und Virenscanner im Blick. Dem Unsicherheitsfaktor Mensch wird hingegen weniger Aufmerksamkeit geschenkt.

„Die IT-Systeme der Firmen können noch so hochgerüstet sein, wenn versäumt wird, die Mitarbeiter für die IT-Sicherheit nachhaltig zu sensibilisieren. Denn dann haben Dritte mehr oder weniger leichtes Spiel, an sensible Daten zu kommen oder sich in die IT einzunisten“, sagt Tobias Flaig, Leiter Infrastructure Services bei der „IT.TEM GmbH“.

Zahlreiche Fehlerquellen

Tobias Flaig ist bei der „IT.TEM GmbH“ Leiter Infrastructure Services. In dieser Funktion führt er für Unternehmen so genannte Awareness-Schulungen zum Thema IT-Sicherheit durch.

Das Stuttgarter Unternehmen bietet spezielle Awareness-Schulungen für Arbeitnehmer an, in denen die Teilnehmer auf klassische Fehler und Fallstricke hingewiesen werden. Und davon gibt es viele: „Das fängt schon damit an, dass Mitarbeiter etwa in der Mittagspause ihren PC-Arbeitsplatz verlassen, ohne den Bildschirm zu sperren. Ein beliebter Klassiker sind zudem scheinbar herrenlose USB-Sticks, die plötzlich im Unternehmen oder auf dem Firmenparkplatz herumliegen. Da ist die Neugier bei Mitarbeitern groß, herauszufinden, welche Daten sich darauf befinden. Was sie nicht wissen: Der Stick ist eine Art Tastatur, die mit Befehlen hinterlegt ist und beim Andocken unbemerkt Aktionen ausführt“, warnt der IT-Experte. Flaig muss zudem immer wieder feststellen, dass privat und geschäftlich die gleichen Passwörter genutzt werden. Das mache es Cyber-Kriminellen besonders leicht, an Zugangsdaten zu kommen. Außerdem sei das Social Engineering nicht zu unterschätzen. Hier werde versucht, unter Angabe einer falschen Identität über soziale Netzwerke wie Facebook Vertrauen zu „schwachen Mitarbeitern“ aufzubauen, um an sensible Informationen zu kommen. „Generell muss man sagen, dass sich Mitarbeiter und Unternehmensleitung zu sehr auf die Technik verlassen und viel zu zögerlich reagieren, wenn etwas im System plötzlich nicht mehr rund läuft – ganz nach dem Motto: ‚Es wird schon alles sicher sein.‘ Doch jeder muss sich bewusst sein, dass Hacker in diesem Katz-und-Maus-Spiel etwa mit den Herstellern von Antiviren-Programmen immer die Nase vorne haben werden, letztere immer nur auf Vorkommnisse reagieren können“, mahnt Flaig.

Neue Gefahren durch mobiles Arbeiten

Mit der Zunahme des mobilen Arbeitens müssen sich die Unternehmen mit weiteren Risiken auseinandersetzen und ihre Mitarbeiter entsprechend sensibilisieren. Egal ob man Zuhause oder unterwegs arbeitet – der Experte rät, immer über eine VPN-Leitung verschlüsselt zu agieren. Hingegen entpuppe sich das augenscheinlich sichere Heimnetzwerk immer öfter als Einfallstor für Hacker. Sie würden sich beispielsweise über alte und schlecht geschützte Smarthome-Geräte wie Fernseher sehr leicht Zutritt verschaffen. Vorsicht ist auch außerhalb der eigenen vier Wände geboten: „Wer unterwegs statt VPN öffentliche Hotspots nutzt, muss sich stets bewusst sein, dass man einen Hotspot-Zugang benennen kann, wie man will. Da gibt es keinen Sicherheitsmechanismus, der dessen Echtheit überprüft.“ Um die Sicherheit im öffentlichen Raum weiter zu erhöhen, empfehlen sich laut dem Experten so genannte Privacy-Screen-Folien, die auf dem Bildschirm eines Laptops oder Tablets aufgebracht werden und ein seitliches Einsehen verhindern. Wer dann noch die Daten auf den Endgeräten verschlüsle, sei unterwegs vor den größten Risiken geschützt.

Schockmomente bleiben im Gedächtnis

Im Rahmen der Awareness-Schulungen von „IT.TEM“ werden die Teilnehmer sehr praxisnah an die Thematik herangeführt. „Wir zeigen anhand von Live-Präsentationen sehr anschaulich, wie einfach es manchmal ist, an sensible Daten zu gelangen. Die Teilnehmer sind jedes Mal regelrecht schockiert, wenn sie sehen, wie einfach es zum Bespiel ist, innerhalb von fünf Minuten einem älteren Windows-System das Passwort zu entlocken. Solche Schockmomente bleiben im Gedächtnis haften.“ Damit das Thema eine gewisse Nachhaltigkeit im Unternehmen entwickelt, haben sich laut Flaig regelmäßig stattfindende kurze Pitches im Berufsalltag bewährt, in denen Mitarbeiter zusammen mit den IT-Verantwortlichen und der Geschäftsleitung „aktuelle heiße Themen“ rund um die IT-Sicherheit diskutieren und besprechen. „Unsere Erfahrung hat gezeigt, dass ein solches Format von den Mitarbeitern sehr geschätzt wird und ihnen Sicherheit im Umgang mit Risiken gibt. Hingegen haben sich Security-Newsletter, die in der heutigen E-Mail-Flut untergehen, nicht bewährt.“ Ein Thema liegt Flaig noch besonders am Herzen: „Ein Mitarbeiter, der in eine Cyber-Security-Falle getreten ist, wird sich naturgemäß damit schwer tun, das Vorkommnis zu melden und einen Fehler einzuräumen. Daher obliegt es der Geschäftsführung, Ängste abzubauen und Stigmatisierungstendenzen frühzeitig zu unterbinden. Denn in vielen Fällen unterlaufen Mitarbeitern die Fehler trotz bestem Wissen und Gewissen. Die Fehler sind in der Regel nicht in der Person des Mitarbeiters, sondern in der Raffinesse von Hackern & Co. zu suchen.“ ■ *-hf*

► www.it-tem.de