MODERNE SICHERHEITSKULTUR GEGEN HACKER-ANGRIFFE

von Christine Kipke

Kriminelle zielen mit ihren digitalen Attacken längst nicht mehr auf die Systeme eines Unternehmens allein. Zunehmend geraten die Angestellten unter Beschuss, weil sie als schwächstes Glied in der Kette gelten. Sie werden Opfer eines CEO-Fraud, Phishing-Angriffs oder einer Social-Engineering-Kampagne und öffnen Verbrechern Tür und Tor des Unternehmens, ohne sich dessen bewusst zu sein – oder sich wirklich schuldig zu machen. Fällt Hackern das Firmen-Email-Konto eines Mitarbeiters in die Hände, weil sie zuvor eine geschickte Social-Engineering-Attacke mit einem Phishing-Angriff kombiniert haben, darf nicht die Schuld beim Angestellten gesucht werden. Fällt er auf solche Betrügereien herein, sollte vielmehr die Führungsebene zu der Einsicht gelangen, dass ihrer Organisation etwas Entscheidendes fehlt: eine moderne Sicherheitskultur.

Die Mitarbeiter sind Menschen und machen eben ab und an Fehler. Dem aber sollte ein Unternehmen entgegenwirken, um seinen Angestellten den Druck oder die Angst zu nehmen, das Opfer eines schädigenden Cyberangriffes zu werden. Der Slogan muss lauten, die Mitarbeiter zu einer «menschlichen Firewall» auszubilden, damit sie nicht mehr das schwächste Glied in der Kette darstellen, sondern effektiv dazu beitragen, die Firma – und sich selbst – vor gefährlichen Bedrohungen zu schützen. Um eine Sicherheitskultur zu etablieren, müssen aber alle Abteilungen Hand in Hand arbeiten. Das fängt oben in der Geschäftsführung an. Sie muss mit gutem Beispiel vorangehen. Dazu gehört das richtige Verhalten gegenüber virtuellen Bedrohungen vorzuleben und präventive Massnahmen zu ergreifen wie auch zu ermöglichen. Zudem muss sie sich verantwortlich fühlen, falls doch ein Zwischenfall geschieht, denn tatsächlich haftet in einem solchen Fall die Geschäftsführung, nicht die Buchhalterin, die aufgrund mangelnder Vorkehrungen zum Opfer wurde. Gerade Letzteres sollten sich moderne Arbeitgeber stets ins Bewusstsein rufen.

Schulungen bieten sich als einfache und wirkmächtige Lösung an, um das Unternehmen mit einer modernen Sicherheitskultur zu stärken. Das Stichwort «Security Awareness» steht im Mittelpunkt. Es ist unabdinglich, dass Menschen heutzutage eine gewisse Aufmerksamkeit für digitale Gefahren entwickeln müssen, wenn sie mit digitalisierten Geräten hantieren. Dieses Bewusstsein zu erhöhen und die Feinheiten zu vermitteln, anhand derer sich auch ausgeklügelte Betrugsversuche erkennen lassen, ist das Ziel umfangreicher Trainings. Diese sollten aber nicht staubtrocken sein und aus dem langatmigen Durchwälzen von Anleitungen bestehen, oder mit dem erhobenen Zeigefinger durchgeführt werden. Vielmehr muss der Spass beim Lernen im Vordergrund stehen und am besten lassen sich die Botschaften sogar auf individuelle Lernbedürfnisse zuschneiden.

Besonders einfach zu verwalten sind die Trainings natürlich, wenn sie auf einer Plattform zusammenfliessen, von wo sie gestartet und die Ergebnisse überwacht werden können. Auf diese Weise lassen sich verschiedene Aspekte der Security Awareness gezielt simulieren und einüben, sodass ein einheitliches Bild vom Wissensstand der Mitarbeiter entsteht. Kontinuierliches Training und die Erkenntnisse über einen längeren Zeitraum zu testen, vertieft das Wissen, sodass bestimmte Abläufe und Warnungen für die Angestellten zur Routine werden und sie reale Gefahrensituationen spielend meistern. Ist dies erreicht worden, dann kann von einer echten Sicherheitskultur in einem Unternehmen gesprochen werden, die sich über einen längeren Zeitraum aufgebaut und gefestigt hat. ●

CHRISTINE KIPKE

ist Managing Director bei KnowBe4.

www.knowbe4.de