Der Mensch als schwächstes Glied der Security-Kette

Hacker haben heute mehr und grössere Angriffsflächen als je zuvor – dies auch wegen unvorsichtigen Mitarbeitenden. Wie kann man allen Unternehmensmitgliedern beibringen, dass sie die Security-Richtlinien akzeptieren?

In Bezug auf Cyber-Security hat sich in den letzten Jahren ein Wandel vollzogen: Wurden Unternehmensnetzwerke früher vom Chief Security Officer als abzuschottende Burg betrachtet und gegen Gefahren von aussen verteidigt, führt die zunehmende Verschmelzung der privaten und geschäftlichen Welt dazu, dass die Integration von privaten IT-Geräten der Mitarbeitenden in Sicherheitskonzepte von Unternehmen notwendig wird. Da von unterschiedlichen Geräten und nicht selten auch von überall auf der Welt aus auf das Firmennetzwerk zugegriffen werden soll, wurde die Infrastruktur der meisten Unternehmen in den letzten Jahren komplexer als je zuvor. Dadurch ergeben sich für Cyber-Kriminelle mehr und grössere Angriffsflächen. Dazu kommt, dass weltweit heute schätzungsweise drei Milliarden Geräte mit Malware infiziert sind, bis 2020 sollen es gar 25 Milliarden Geräte sein.

Unternehmen müssen bei ihren Sicherheitskonzepten nicht nur zahlreiche Geräte, Netzwerke und Applikationen berücksichtigen. Das schwächste Glied in der Security-Kette ist meistens der Mensch. Es dauert durchschnittlich 200 Tage bis Cyber-Angriffe auf Firmen oder Organisationen bemerkt werden. Man kann aber nicht den Durchschnitt aller Bestandteile der Kette berechnen, vielmehr ist das gesamte Security-Konzept weniger stark als das schwächste Glied. Deswegen sollten sämtliche Mitarbeitende auf die Themen Hacker-Angriffe, Phishing und Sicherheit sensibilisiert werden. Ein Chief Security Officer oder die IT-Abteilung dürfen künftig nicht mehr die ganze Verantwortung alleine tragen.

Sicherheitskonzept muss zur Unternehmenskultur passen

Wie mit Security-Programmen und -Regeln umgegangen wird, hängt letzten Endes stark von der Unternehmenskultur ab. So ist es möglich, dass eine Standard-Software und ein allgemein akzeptiertes Regelwerk in einer Firma ausreichen, während sich die Angestellten eines anderen Betriebs schwer tun damit, grundlegende Sicherheitsprinzipien zu befolgen und aus diesem Grund umfassendere Vorgaben und Schulungen benötigen. Wird beispielsweise eine Sicherheitsrichtlinie von den Angestellten konsequent missachtet, bietet es sich an, dieses Verhalten beim Aufstellen neuer Regeln in Betracht zu ziehen, damit die finale Lösung von der ganzen Unternehmung akzeptiert wird.

Es ist empfehlenswert, mit einem erfahrenen Security-Partner zusammenzuarbeiten, der an Unternehmensbedürfnisse angepasste Sicherheitslösungen anbietet und das Nutzungsverhalten der Mitarbeitenden berücksichtigt.

Autor: Andre Keller ist Head of Cyber Security bei Atos in der Schweiz, einem führenden Anbieter von digitalen Services. Weitere Informationen unter www.ch.atos.net