Unternehmen verschlafen Sicherheitslücken

Die Zahl von Cyber Security Incidents erhöht sich stetig und parallel dazu nehmen die Bedürfnisse nach umfangreichen Absicherungen zu. Thomas Masicek, Head of Portfolio Unit Security T-Systems Alpine, gibt einen Überblick über aktuelle Bedrohungen und wie man sich am besten darauf vorbereitet.

Herr Masicek, was ist die grösste Sicherheits-Schwachstelle eines Unternehmens?

Thomas Masicek: Eine sehr grosse Gefahr für Unternehmen ist nach wie vor der Faktor Mensch. Denn warum gelingen zielgerichtete Angriffe? Zu 80 Prozent deshalb, weil eine grosse Anzahl vertrauenserweckender E-Mails verschickt wird und ein Mitarbeitender klickt darauf – und schon ist eine Schadsoftware auf dem Rechner platziert. Es ist derzeit leider noch nicht möglich, jedes einzelne Gerät im Unternehmensnetzwerk komplett sicher zu halten. Es gibt immer Schwachstellen in Computersystemen. Dazu kommt, dass Unternehmen die Netzwerke teilweise auch nur halbherzig konfigurieren. Die meisten Unternehmen sind damit überfordert, die Geräte auf dem aktuellen Stand zu halten und verschlafen so wichtige Sicherheitslücken.

Wie können sich Unternehmen besser schützen?

Es ist erforderlich, dass sich die Unternehmen viel mehr mit dem Thema Sicherheit auseinandersetzen. Die IT-Abteilungen müssen ihre Hausaufgaben machen und die im Einsatz befindlichen Geräte ordnungsgemäss konfigurieren und warten. Wir sehen das auch bei den Projekten, die wir aktuell durchführen. Da geht es einerseits sehr stark in Richtung Awareness-Training, also wie kann ich Mitarbeiter schulen, dass sie Gefahren erkennen, zum Beispiel auch mit Gamification. Darüber hinaus gehören Social Engineering-Tests und Phishing-Kampagnen dazu, die wir ausschicken und anhand deren man den Mitarbeitenden erklären kann, was kritisch ist. Sie lernen also praxisnah.

Ein weiterer Bereich ist das Erkennen von Angriffen. Dafür gibt es das sogenannte Security-Information-Event-Management-System (SIEM), dass alle möglichen Informationen eines Netzwerks sammelt. Ein Security-Operation-Center (SOC) kann damit eventuelle Alarme analysieren und den Kunden darauf hinweisen, dass eine Anomalie vorherrscht, und im Bedarfsfall auch gleich reagieren.

Thomas Masicek, MSc., CISSP

1976 geboren | Studium für Information Security Management an der Universität Krems | 2000–2002 T-Mobile Austria GesmbH als Teamleiter Internet Services/ IT Security Management | seit 2002 T-Systems Austria GesmbH in unterschiedlichen Funktionen im Security Management, ab 2009 Chief Security Officer AT, ab 2012 als Head of Security Management und ab 2018 als Head of Portfolio Unit Cyber Security Austria & Switzerland.

Welche Herausforderungen gibt es für Unternehmen beim Thema Security und Datenschutz?

Verordnungen wie das Schweizer Datenschutzgesetz, die DSGVO und neue Richtlinien führen zum Problem, dass Unternehmen nicht mehr in der Lage sind, selbst das gesamte Anforderungskonvolut korrekt steuern und bewerten zu können. Wir haben mit der GRC-Cloud (Governance, Risk und Compliance) ein System entwickelt, das Unternehmen dabei unterstützt, ihr Sicherheitsmanagement weltweit zu steuern, zu kontrollieren und zu reporten. Wir bieten etwa für den Finanzbereich, den Gesundheitsbereich oder für Betreiber kritischer Infrastrukturen spezielle Ableger der Lösung an, in denen die entsprechenden Kontrollkataloge, Prozesse und Workflows definiert sind, sodass das Unternehmen eigentlich nur mehr diese Plattform nutzen muss. Sie weist darauf hin, wann etwas zu tun ist, und sie leitet durch den Workflow. Am Ende des Tages hat man dadurch die Sicherheit, nichts vergessen zu können. Das bedeutet, ich bin jederzeit in der Lage, meine Investments ganz zielgerichtet einzusetzen.

Was können Unternehmen unmittelbar für mehr Security tun?

Was wir bei Security Audits oft feststellen, ist, dass Unternehmen viel Geld in den Bereich Security investieren, aber teilweise wirkungslos. Da gibt es zum Beispiel mehrstufige Firewall-Konzepte, aber keine davon ist richtig konfiguriert. Und daneben gibt es den absolut ungeschützten Endpoint wie einen Laptop, der für einen Angreifer ein viel leichteres Target ist. Das bedeutet, ein Unternehmen muss wissen, welcher Bedrohung es aktuell ausgesetzt ist, wo es angreifbar ist und welche Massnahmen es für den Ernstfall braucht. ■

T-Systems Schweiz AG, CH-3052 Zollikofen
✆ +41 (0) 848 11 12 11
info@t-systems.ch, www.t-systems.ch