IHK Niederbayern

NIEDERBAYERISCHE WIRTSCHAFT

Das IHK-Magazin · 12/2019

Digitalisierung

Schutz gegen Cyber-Attacken

LEINWANDHELD
Die Citydom Straubing GmbH & Co. KG lässt Kinoträume wahr werden

PRÜFUNGSBESTE
248 Einser-Azubis aus Niederbayern ausgezeichnet

STEUERÄNDERUNGEN
Praxisrelevante Neuerungen im Steuerrecht für 2020

Obwohl die perfiden Methoden der Cyber-Kriminellen inzwischen durchaus bekannt sind, fallen immer noch Menschen auf deren Tricks herein. Umso wichtiger sind der Schutz mobiler Endgeräte und die Umsetzung von Präventionsmaßnahmen. Gar nicht so einfach, denn Mobilgeräte sind zum einen in ihrer Nutzung und Technologie sehr dynamisch und zum anderen gibt es eine Vielfalt und -zahl an Möglichkeiten, Anwender zu manipulieren. Erschwerend kommt hinzu, dass viele Anwender eine emotionale Bindung zu ihren Smartphones haben und deshalb mit ihrem Handy sehr unbekümmert umgehen und Einschränkungen nur widerwillig akzeptieren.

Nischenlösungen vertrauen

Dabei gibt es gute Lösungsanbieter, die diese Aspekte berücksichtigen. Deren Manko ist allerdings, dass es sich oft um Nischenlösungen innovativer Unternehmen handelt, die wenig bekannt sind. IT-Verantwortliche sollten sich intensiv mit dem Angebot solcher Security-Lösungen beschäftigen, bevor sie sich für ein System entscheiden.

Um außerdem langfristig eine Bewusstseinsänderung herbeizuführen, ist zunächst eine grundsätzliche Analyse der im Einsatz befindlichen Technologien und der Security-Strategien notwendig. Man muss sich die Frage stellen, welche Daten es gibt und wie kritisch deren Verlust ist. Aspekte wie BYOD, COPE, DSGVO und besonders die Usability müssen dabei unbedingt berücksichtigt werden. Dann geht es an die Erstellung eines gesamtheitlichen Sicherheitskonzepts „Gerät – Daten – Apps – Traffic". Hier spielt zunächst einmal das Smartphone sowie dessen technische Konfiguration und zur Verfügung stehender Content eine wichtige Rolle. Ein besonderes Augenmerk sollte auch dem Schutz der Apps und dem Traffic gelten. Da geht es etwa um Fragen, welcher Content in welcher Situation konsumiert werden darf oder wie sich Daten vor Man-in-the-Middle-Attacken sowie auf dem Weg zwischen Sender und Empfänger schützen lassen.

Digitale Aufklärung

Auch mit modernsten Security-Lösungen und strengen Vorgaben lassen sich IT-Systeme allerdings nicht vollständig schützen. Deshalb müssen die Unternehmen ihre Mitarbeiter kontinuierlich aufklären und schulen – am besten, indem sie Mitarbeiter auch mit der Methodik und den Folgen von Social Hacking durch simulierte Cyber-Attacken konfrontieren. Je plakativer dabei die Tricks der Betrüger beschrieben werden, umso wirkungsvoller ist der Lerneffekt. Jeder, der schon einmal erlebt hat, wie es ist, wenn er keinen Zugriff mehr auf sein Smartphone hat, vom Konto unautorisierte Überweisungen getätigt wurden oder sein Smartphone über ein manipuliertes öffentliches WLAN gehackt wurde, wird das so schnell nicht vergessen und zukünftig sein Handeln überdenken.

Michael Krause, TAP.DE Solutions GmbH