Rien ne va plus

#Mobile-Threat-Prevention, #Cyber-Security, #Datensicherheit, #Sicherheitskonzepte

Michael Krause ist Geschäftsführer der **TAP.DE Solutions GmbH**, ein Beratungsunternehmen, das sich mit Themen wie Sicherheit, Prozesseffizienz, dem Arbeitsplatz der Zukunft, Endpoint Security, Service Management und Compliance beschäftigt. Um den Spagat zwischen der Erwartungshaltung von Anwendern und IT zu überwinden, entwickeln die Consultants von TAP.DE ganzheitliche Konzepte und Lösungen und agieren zudem als fachkundiger Systemintegrator.

www.tap.de

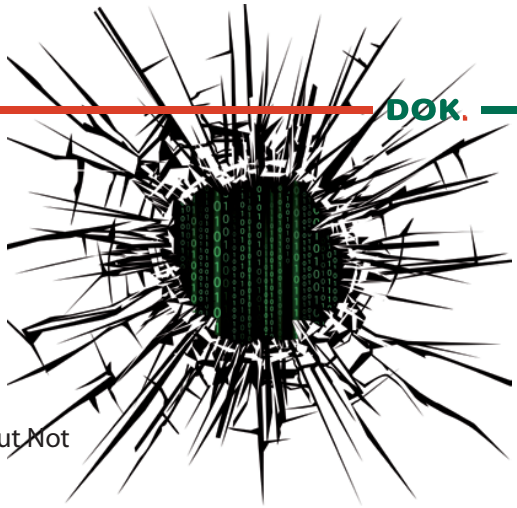
In Sachen Datensicherheit ist vorausschauendes Handeln das A und O. Die größte Herausforderung sind dabei aber keineswegs nur die technischen Aspekte, sondern sie liegt vielmehr in der Sensibilisierung der Mitarbeiter. Der Grund sind ihre Smartphones am Arbeitsplatz: Denn zum einen haben die Nutzer zu ihrem Smartphone in der Regel eine durchaus emotionale Bindung und zum anderen sind sich nur wenige bewusst, wie leicht ein solches Gerät gehackt werden kann. Ein Spannungsfeld, das den Schutz von Mobilgeräten überaus komplex macht.

Zwar sind die verschiedenen Methoden wie Phishing, Tailgating, Whaling oder andere mittlerweile weitreichend bekannt, aber es fallen immer noch genügend Menschen auf die perfiden Tricks der Cyberkriminellen herein. Umso wichtiger ist der Schutz mobiler Endgeräte und so wundert es kaum, dass der Ruf nach Mobile Threat Prevention immer lauter wird.

Warum aber tun sich viele Organisationen mit dem Schutz ihrer Mobilgeräte so schwer? Warum fokussieren sie sich nach wie vor auf die Sicherheit von Computern und Rechenzentren, obwohl sie es längst besser wissen müssten? Weil Mobilgeräte zum einen in ihrer Nutzung und Technologie sehr dynamisch sind und es zum anderen eine Vielfalt an Attacken gibt, denen es gelingt, die Anwender zu manipulieren. Es ist erschreckend, dass gerade CEOs Hunderte von Apps auf ihren Smartphones haben, mit denen sie Kriminellen Tür und Tor öffnen; kein Wunder, denn gerade die hochsensiblen Daten von Führungskräften sind äußerst lukrativ für die Angreifer.

Nischenlösungen Vertrauen schenken

Problematisch ist dabei, dass viele Anwender und folglich auch Mitarbeiter sehr unbekümmert mit ihrem Smartphone umge-



hen und Einschränkungen ihres Arbeitgebers nur widerwillig akzeptieren. Dabei gibt es bereits sehr gute Lösungen, die diese Aspekte berücksichtigen. Allerdings stammen diese Angebote oftmals von kleinen, aber sehr innovativen Nischenunternehmen, die in der Öffentlichkeit nur wenig bekannt sind und die deshalb nur eine geringe Akzeptanz haben.

Erschwerend kommt hinzu, dass IT-Administratoren diese Lösungen nicht nur nicht kennen und finden, sondern dass sie auch noch den Mut haben müssen, sie einzusetzen. Dass es sich zudem häufig um Cloud Services handelt, weil sich diese den dynamischen Cyberangriffen besser entgegenstellen können, ist ein weiterer Malus im System – Stichwort Compliance und DSGVO. Voraussetzung für mehr Sicherheit der Mobilgeräte sind hier aber eine grundlegende Bewusstseinsänderung und ein mutiger Perspektivwechsel.

Kombination aus Usability und Security

Damit dieser Wandel überhaupt erst einmal in Gang kommt, ist es wichtig einschätzen zu können, welche Bedeutung Mobile Threats innerhalb eines Unternehmens überhaupt haben. Im ersten Schritt ist deshalb eine grundsätzliche Analyse der im Einsatz befindlichen Technologien bzw. Strategien notwendig. Besonders wichtig ist dabei ein Blick auf die Anforderungen seitens der Business-Perspektive: Man muss sich die Frage stellen, welche Daten es gibt und wie kritisch deren Verlust wäre. Aber auch die Wünsche der Anwender spielen eine wichtige Rolle; diese sollten bei der Umsetzung eines Sicherheitskonzepts entsprechend berücksichtigt werden, etwa indem sich ein Unternehmen hinsichtlich BYOD öffnet und eine Kombination aus Usability und Security findet.

Wesentlich bei der Erstellung eines solchen Konzepts ist deshalb die Berücksichtigung vier verschiedener Anforderungsebenen. Dazu zählt zunächst einmal das Mobilgerät an sich sowie dessen technische Konfiguration. Hinzu kommt der Content, auf den das Gerät Zugriff hat bzw. den der Anwender benötigt, um mobil produktiv zu sein. Untersucht werden muss, ob unternehmensinterne Daten betroffen sind und wie es mit deren Offline-Replikation aussieht. Besonderes Augenmerk gilt dem Schutz der Apps, die auf dem Gerät verwendet werden. Aber auch den Traffic darf man nicht vergessen. Hier geht es um die Frage, in welcher Situation was konsumiert werden darf und wie sich das Gerät und die Daten vor Man-in-the-Middle-Attacken, etwa durch Phishing-Kampagnen, schützen lässt. Daten werden auf Containern geschützt, aber was passiert mit diesen auf dem Weg in den Container bzw. von dorthin zum Empfänger?

Aufklärung tut Not

Man kann es drehen und wenden wie man will: Auch mit den modernsten Sicherheitsvorkehrungen und den strengsten Vorgaben in Bezug auf den Datenschutz lassen sich IT-Systeme nie vollständig absichern. Deshalb kann nur eine Kombination der verschiedenen Aspekte und Sicherheitsebenen für bestmögliche Sicherheit sorgen – und das auch immer nur für einen begrenzten Zeitraum.

Fakt ist aber auch, dass jede IT-Infrastruktur, unabhängig davon, wie gut sie geschützt ist, immer nur so valide ist, wie ihr schwächstes Glied: der Anwender. Umso wichtiger ist es, ihn und seine Bedürfnisse ernst zu nehmen und über die Gefahren aufzuklären. Dabei sollte man sein individuelles und sehr emotionales Verhältnis zu seinem Smartphone im Hinterkopf behalten.

Dennoch kommt kein Unternehmen umhin, seine Mitarbeiter aufzuklären und zu schulen. So sieht das auch Volker Bentz, Geschäftsführer von Brandmauer IT. In seinen Augen ist es die einzige Lösung, den Mitarbeitern mit Hilfe von Schulungen und Security Awareness Trainings auf solche Angriffsszenarien vorzubereiten. Nur so können diese einen Social-Hacking-Angriff rechtzeitig identifizieren und richtig handeln. Bentz schlägt vor, im Vorfeld mittels eines simulierten Angriffs herauszufinden, wie Mitarbeiter in solchen Fällen reagieren und wo die Sicherheitslücken genau liegen. [1] Je plakativer dabei die Tricks der Betrüger und die Folgen der Cyberattacken für den Anwender und das Unternehmen beschrieben werden, umso wirksamer ist der Lerneffekt.

Fazit

Jeder, der schon einmal erlebt hat, wie es ist, wenn er auf einmal keinen Zugriff mehr auf sein Smartphone hat, der gesehen hat, wie leicht sich öffentliche WLANs manipulieren lassen und gespürt hat, wie verheerend Man-in-the-Middle-Attacken sind, wird diese Erfahrung so schnell nicht mehr vergessen. Deshalb sollte man den Spieß umdrehen und die emotionale Nähe der Anwender zu ihrem Smartphone nutzen, um sie zu sensibilisieren. Zu ihrem eigenen und zum Schutz der Unternehmen.

Referenzen

[1] https://www.brandmauer.de/blog/it-security