KOMMENTAR

Es muss immer erst einmal was passieren

***NACH WIE VOR IST DAS MOBILE DEVICE** für Sicherheitsbedrohungen das Einfallstor Nummer eins. Dennoch wird das Thema „Mobile Security" von deutschen Unternehmen weitestgehend ignoriert. Grund hierfür ist oft die Angst, dass persönliche Daten oder das Nutzungsverhalten ausgelesen werden. Laut Michael Krause von Tap.de kann diese Situation zum Verlust von Know-how und – damit verbunden – zum Verlust des Technologievorsprungs führen.*

IMMER ÖFTER HÖRT MAN von erfolgreichen Cyberattacken, oft von Hackern aus dem Ausland. Erst vor kurzem gelang es Kriminellen, sog. „Black Hats", die IT des Traditionsjuweliers Wempe lahm zu legen und ein Lösegeld zu erpressen. Wempe teilte nach diesem Angriff mit, dass es seine IT-Infrastruktur modernisieren und das Sicherheitskonzept bearbeiten werde. Wie es den Cyberkriminellen gelingen konnte, in das System einzudringen, wurde nicht kommuniziert; es ist jedoch wahrscheinlich, dass auch mobile Geräte involviert waren. In diesem Fall wurde zwar kein Technologiefachwissen abgegriffen, aber der Imageverlust ist durchaus hoch.

Michael Krause ist Geschäftsführer des Sicherheitsanbieters Tap.de Solutions.

Dringender Handlungsbedarf

Viele Unternehmen glauben, dass ihr Mobile Device Management (MDM) automatisch auch für eine ausreichende Absicherung der Mobilgeräte sorgt, sind sich aber auch nicht wirklich sicher. Die Zweifel der verantwortlichen IT-Spezialisten sind berechtigt, werden aber von den Entscheidungsträgern nicht ausreichend priorisiert. Zwar kennt man in Fachkreisen die verschiedenen Angriffsmethoden wie Phishing, Tailgating, Whaling etc.; die Unternehmen schützen ihre Anwender aber nicht vor diesen perfiden Tricks. Helfen kann hier ganz einfach der Einsatz einer Mobile-Threat-Prevention-Lösung (MTP). Eine solche Lösung ist schnell und unkompliziert per Cloud-Dienst aktivierbar und sorgt dafür, dass einerseits die Daten und andererseits das Gerät sofort abgesichert sind.

Voraussetzung ist, dass IT-Verantwortliche die fatalen Folgen mangelnder Schutzmechanismen aufzeigen. Die DSGVO und auch die hohen IT-Sicherheitsanforderungen für die Betreiber kritischer Infrastrukturen schaffen die Grundlage, diese dringend notwendigen Security-Maßnahmen beim Management zu platzieren und durchzusetzen.

MOBILE THREAT PREVENTION

Moderne MTP-Lösungen können Unternehmen vor Sicherheitsbedrohungen schützen:

- **Datenverlust**
- **Social Engineering**
- **Wi-Fi-Interferenz**
- **Veraltete Geräte**
- **Kryptojacking-Angriffe**
- **Geräteverlust**

Am abschreckenden Beispiel eines Hardware-Herstellers lässt sich aufzeigen, welche Folgen mangelnde Datensicherheit haben kann. Gelingt es Cyberkriminellen, die IT eines Hardware-Herstellers, der von ein bis zwei Prozent Marge lebt, zu kapern, kann dies für dessen Business tödlich sein. Denn sollten bei diesem Angriff personenbezogene Daten betroffen sein, darf laut DSGVO eine Strafe von bis zu fünf Prozent des Jahresumsatzes veranschlagt werden – eine Summe, die das Unternehmen möglicherweise in die Insolvenz treibt.

Um derartige Horrorszenarien zu vermeiden, ist dringend eine Bewusstseinsänderung notwendig. Unternehmen müssen die im Einsatz befindlichen Technologien bzw. Strategien und ihre Wirkungskraft unter Berücksichtigung der aktuellen Bedrohungslage analysieren. Mitarbeiter müssen mithilfe von Schulungen und Security-Awareness-Trainings über solche Bedrohungen aufgeklärt und entsprechend sensibilisiert werden. Sicherheitsexperten empfehlen sogar, Social-Hacking-Angriffe zu simulieren, um herauszufinden, wie Mitarbeiter in solchen Fällen reagieren.

Oft versteckt sich hinter einer SMS mit einer Gewinnbenachrichtigung oder einem kostenlosen WLAN-Hotspot ein ausgeklügelter Cyberangriff. Auf solche und ähnliche Gefahren müssen Benutzer aufmerksam gemacht werden, diese als Gefahr erkennen und entsprechend reagieren. Folgenschwere Cyberhacks bei Unternehmen wie Wempe oder auch Angriffe auf die mobilen Geräte von Mitarbeitern sollten Warnung genug sein, das Thema „Mobile Security" mit der erforderlichen Ernsthaftigkeit voranzutreiben. Das Prinzip Hoffnung sollte längst ausgedient haben – Anwender müssen mit längst vorhandenen und bewährten Technologien geschützt werden!