KOOPERATION

Wie sicher sind mobile Geräte?

Smartphones und Tablets im Geschäftsumfeld geraten immer öfter ins Visier von Hackern. Beim IT-Sicherheitstag am 29. November 2016 in Kempten diskutieren Experten über die wirksamsten Lösungen.

Im Alltag funktioniert die klare Trennung von Arbeitszeit und Freizeit oft nicht mehr. Durch immer mehr mobile Geräte kann außerhalb von Büros und Werkhallen gearbeitet werden, und immer öfter nutzen Mitarbeiter auch private Geräte im Job oder verwenden private Apps geschäftlich. Wie lässt sich der „mobile Gerätezoo" überhaupt noch managen und verantworten? Für Unternehmen ergeben sich dabei viele Fragen.

Mit dem IT-Sicherheitstag „Mobile Security – Sicherheit für mobile Lösungen" am 29. November 2016 in Kempten sollen Unternehmen für die Gefahren sensibilisiert werden. Bei der Kooperationsveranstaltung der IHK Schwaben mit dem Branchennetzwerk aitiRaum präsentieren Experten von Hochschulen, erfahrene Praktiker und Fachleute führender Unternehmen konkrete Ansätze und Lösungen, die Mobilität ermöglichen und trotzdem Sicherheit bieten. Die BSW interviewte Experten des aitiRaums zu aktuellsten Fragen.

BSW: Warum sollten sich Arbeitgeber gut überlegen, ob sie damit einverstanden sind, dass Beschäftigte ihre eigenen Geräte dienstlich nutzen?

Birgit Maneth, Rechtsanwältin Lutz, Abel Rechtsanwälte GmbH

Für die Nutzung von Daten, Software und Geräten eines Unternehmens gibt es klare Regeln, die dem Unternehmen den Schutz gegen Missbrauch oder Verlust ermöglichen. Diese Regeln funktionieren nicht bzw. nur eingeschränkt, wenn sich Unternehmensdaten auf dem privaten Endgerät eines Mitarbeiters befinden. Denn in diesem Fall kollidiert das Privateigentum des Mitarbeiters am Gerät mit den Unternehmensrechten an den gespeicherten Daten. Ein erhebliches Risiko und Konfliktpotenzial: Der Arbeitgeber bleibt für die Sicherheit und Vertraulichkeit der Daten verantwortlich, muss einem Mitarbeiter also Regeln zur Nutzung eines Privatgerätes auferlegen. Diese sind manchmal auch nur schwer umsetzbar für den Mitarbeiter, zum Beispiel ein Verbot bestimmter Apps oder keine Nutzung durch Lebenspartner. Ein verantwortungsbewusster Geschäftsführer oder Inhaber wird diese Regeln gleichwohl definieren und die Einhaltung für alle Mitarbeiter festschreiben. Tut er das nicht, kommt er relativ leicht mit geltendem Recht in Konflikt und riskiert empfindliche Strafen.

BSW: Worauf müssen Unternehmen bei Mobile Security besonders achten?

Christian Köhler, Fly-Tech IT GmbH & Co. KG

Mobile Geräte und Anwendungen existieren nicht autark, das heißt, sie müssen in die IT-Architektur des Unternehmens passen, administrierbar sein und Anforderungen erfüllen und den Nutzern echte Vorteile bringen. Auch wenn ein gewisser Mehraufwand nicht vermeidbar ist, müssen sich die Kosten und der Aufwand in Grenzen halten und kalkulierbar sein.

Unterschiedliche Systeme und Lösungen können bei der Erfassung, Dokumentation und dem Management mobiler Geräte unterstützen, damit effizientes Arbeiten auch ohne zu hohem Aufwand in der IT-Abteilung ermöglicht wird. Wichtig ist, sicherheitsrelevante Mechanismen und Prozesse im Unternehmen zu schulen, für die Nutzung zu sensibilisieren und die Einhaltung auch zu prüfen und zu überwachen. Nur ein ganzheitlicher Ansatz, der Geräte, Anwendungen und den Nutzer umfasst, kann eine Lösung darstellen.

BSW: Warum sind Apps ein besonderes Sicherheitsrisiko?

Dr. Ekkhard Schnedermann, Schnedermann Software Consulting GmbH

Was Apps oft besonders interessant macht, ist der hohe Nutzen durch die unmittelbare Verfügbarkeit von unterschiedlichen Informationen. Das Risiko entsteht durch die Verknüpfung von eigenen Daten mit fremden Diensten, zum Beispiel von einem Termin und persönlichen Daten mit einer Routenplanung. Oder auch die Auswertung von Daten aus GPS, Bewegungssensoren, Kameras oder Wearables durch einen Internetdienst. Wer sich in den Einstellungen des Smartphones die Zugriffsmöglichkeiten seiner Apps ansieht, wird schnell verstehen, warum hier besondere Risiken drohen.

Leider wird über die Experimentierfreude oder die Bequemlichkeit oft die Sicherheit vernachlässigt. Gerade wenn Daten von Kunden betroffen sein können, sollten Unternehmen aufmerksam werden und für den wichtigsten Anwendungsfall eine sichere Lösung etablieren. Das kann eine Private-Cloud sein oder eine Verschlüsselungslösung auf Basis einer Public-Cloud.

Andrea Henkel

IT-Sicherheitstag: Mobile Security – Sicherheit für mobile Lösungen, 29.11.16, 10 Uhr, bigBox Conferencecenter, Kotterner Str. 6, 87435 Kempten

@ Weitere Informationen und Anmeldung unter www.schwaben.ihk.de, **Nr. 2706258**

Bilder: Privat