Den Fünfer und das Weggli gibt es nicht – auch nicht beim Einsatz von mobilen Geräten in Firmen

Der nachlässige Umgang der Mitarbeiter mit mobilen Geräten gibt in vielen Unternehmen Anlass zur Sorge. Derweil spriessen technische Lösungen und neue Policys aus dem Boden – sie könnten allerdings den Spass an der Benutzung der Geräte genauso verderben wie die damit verbundenen Produktivitätssteigerungen. Simon Zaugg

«Rauchen kann tödlich sein», ist der wohl gängigste Hinweis auf Zigarettenschachteln – häufig gepaart mit unappetitlichen Bildern. Kaum jemand zweifelt heute angesichts der eindeutigen Fakten den Wahrheitsgehalt des Slogans ernsthaft an. Der noch vor einigen Jahrzehnten von der Tabakindustrie verbreitete Mythos, dass Rauchen gesund sein könnte, mutet heute überaus seltsam an. Mehr noch: Nach und nach finden Rauchverbote eine breite gesellschaftliche Akzeptanz.

Dem steht heute eine andere, zunehmend verbreitete Sucht, der Rund-um-die-Uhr-Gebrauch von Smartphones, diametral entgegen: Man ist der Entwicklung gegenüber – auch in Unternehmen – zunehmend positiv eingestellt. Laut einer 2010 publizierten Untersuchung des US-Marktforschers Forrester erhoffen sich Unternehmen vom Einsatz der mobilen Geräte eine erhöhte Produktivität ihrer Mitarbeiter (75 Prozent), raschere Feedbacks und beschleunigte Entscheidungsprozesse (65 Prozent) sowie schneller gelöste interne IT-Probleme oder schneller beantwortete Kundenanfragen (je 48 Prozent). Befragt wurden 2274 Entscheider bei IT- und Telekomunternehmen in Europa und Nordamerika.

Angst vor Datenverlust

Manch einem CIO treiben die vielen neuen mobilen Geräte tiefe Sorgenfalten auf die Stirn. Man fürchtet sich vor dem Verlust sensibler Unternehmens- und Kundendaten, da viele Mitarbeiter jederzeit und überall – insbesondere auf den vielen neuen Smartphones – darauf zugreifen. Gänzlich neu ist dieser Aspekt allerdings nicht, denn auch Notebooks gelten als mobile Geräte. «Der Umgang mit Smartphones ist heute allerdings deutlich fahrlässiger. Notebooks stellen eher noch einen Wert dar, das heisst, man geht sorgfältiger mit diesen um», wendet Christof Dornbierer, CTO beim IT-Security-Spezialisten Adnovum, ein. So würden bereits altbewährte Rezepte wie starke Passwörter und eine Verschlüsselung, die Daten bei verlorenen Smartphones nutzlos macht, sowie die Weisung, möglichst wenige Daten auf den Geräten zu speichern, schon viel bewirken.

Auch der Informationssicherheitsexperte Wolfgang Sidler beschäftigt sich aktuell intensiv mit Mobile Security. Er berät Unternehmen und steckt derzeit mit einigen Kunden in der Evaluationsphase für den Einsatz von mobilen Sicherheitslösungen. Damit gemeint sind etwa Lösungen von Data-Leakage-Prevention-Anbietern, die auch mobile Geräte abdecken. Ein Thema sind auch spezialisierte Mobile-Device-Management-Lösungen wie Mobile Iron, die von Swisscom angeboten

Bildquelle: Fotolia, Montage Netzwoche

wird, oder jene von Good Technologies, die unter anderem der Mobile-Security-Spezialist Keyon propagiert. Im «Magic Quadrant» für Mobile-Device-Management-Software der Marktforscher von Gartner, der Ende April erschien, sind weitere Player wie McAfee, Motorola, Symantec, Sybase und Ubitexx vertreten.

Facebook nein, eigenes Smartphone ja

Sidler stellt insgesamt eine erhöhte Sensiblität für das Thema fest: «Es ist klar erkennbar, dass das Thema Mobile Security in vielen Geschäftsleitungen auf der Prioritätenliste immer höher rückt. Insbesondere ist dies bei Firmen, die wirklich sensible Daten haben, der Fall.» Auch bei Swisscom ist Mobile-Device-Management ein wichtiges Thema, wie Martin Lechmann, Sicherheitsexperte beim Telko, gegenüber der Netzwoche bestätigt: «Viele Unternehmen sind sehr interessiert an unserer Lösung. Insgesamt ist unsere Sales-Pipeline gut gefüllt und wir konnten bereits erste Vertragsabschlüsse feiern.»

Das Risiko der möglichen Verbreitung vertraulicher Daten durch mobile Geräte beschäftigt besonders auch die Banken- und Versicherungsbranche. Anlässlich eines Podiums Mitte Oktober am Informationssicherheits-Kongress Security Zone mit Rainer Kessler (Ex-UBS-IT-Sicherheitschef), James Shira (IT-Sicherheitschef bei Zurich Financial Service) und Dinesh Shah (Head IT-Risk Management bei Swiss Re) an der Security Zone gab der Bring-your-own-Device-Ansatz (BYOD) nebst dem Umgang mit Social Media am meisten zu reden. Während Letztere bei Banken und Versicherungen noch weitgehend gesperrt bleiben – weniger aus Sicherheitsbedenken denn aus befürchteten Produktivitätseinbussen –, zeigen sich die Institute dieser Branchen wesentlich offener gegenüber BYOD. Getrieben sei diese Entwicklung gerade auch durch die Geschäftsleitungen und hohe Kader, die ihre liebgewonnenen mobilen Geräte möglichst frei auch geschäftlich einsetzen möchten und so die IT-Riskmanager zusätzlich unter Druck setzten.

Die Krux mit den Policys

Wenig Ermutigendes für IT-Sicherheitsverantwortliche förderte derweil der Connected World Technology Report von Cisco zutage. Die bei jungen Berufstätigen unter 30 Jahren in 14 Ländern weltweit durchgeführte Umfrage zeigte auf, dass junge Erwerbstätige nicht so sehr auf IT-Sicherheit bedacht sind, wie ihre IT-Verantwortlichen das gerne hätten. Demnach verstossen 70 Prozent zumindest hin und wieder gegen Unternehmensrichtlinien zur IT-Nutzung. 60 Prozent sehen die Sicherung von Geräten und Daten im Unternehmen nicht als ihre Aufgabe an. Obwohl es gemeinhin als bewährte Praxis angesehen wird, geben 19 Prozent der Young Professionals zu, dass sie ihre Passwörter nie ändern.

Trotzdem geben knapp zwei Drittel an, dass sie die Arbeit der eigenen IT-Abteilung respektieren. Das macht deutlich, dass sich aus der Anerkennung für die Arbeit der IT-Abteilung kein hohes Sicherheitsbewusstsein im Hinblick auf die berufliche IT-Nutzung ergibt. 68 Prozent der Young Professionals gaben zudem zu, für Fremde einsehbar mit vertraulichen Firmendaten gearbeitet zu haben. Auch wenn das Sicherheitsdenken noch nicht stark ausgeprägt ist, äusserte über die Hälfte der Befragten das Bedürfnis nach flexiblen Arbeitszeiten und der Möglichkeit des Zugriffs von überall. Weiter denken drei von vier jungen Erwerbstätigen, dass ihr Arbeitgeber ihnen mit Geräten am Arbeitsplatz auch die persönliche Nutzung erlauben sollte.

Noch keine Patentrezepte

Diese Befunde sind für Tom Sprenger, CIO bei Adnovum, Ansporn, «vernünftige» Lösungen für die Zukunft zu finden. Ein Patentrezept hat er allerdings keines: «Heute ist es häufig so, dass IT-Sicherheitsverantwortliche grundsätzlich mal alles sperren, damit sie auf der sicheren Seite sind. Das ist insofern fatal, als dass damit der Nutzen meist unnötig eingeschränkt wird. Insbesondere die Digital-Native-Generation akzeptiert dies nicht mehr. Sie findet immer Wege, die Ein-

schränkungen zu umgehen und leitet zum Beispiel Geschäfts-E-Mails an private Mailadressen weiter oder nutzen Cloud-Services wie Dropbox.» Diese These bestätigte auch das US-Wirtschaftsmagazin The Economist. Die sogenannte «Schatten-IT», die CIOs durch die Aussperrung privater Geräte riskierten, sei zwar nichts grundsätzlich Neues, doch es sind nicht mehr ein paar wenige «geeky rebels», die dies tun, sondern ganze Heerscharen von Smartphone- und Tablet-Nutzern.

Um auf diesen Umstand zu reagieren, gibt es unterschiedliche Strategien im Umgang mit mobilen Geräten. So teilte etwa René Eberhard von Keyon an der Security Zone Unternehmen in drei Gruppen ein: Erstens gebe es jene, die geschäftlich keine Smartphones einsetzten. Die zweite Gruppe stellt den Mitarbeitern ein mobiles Gerät zur Verfügung und kontrolliert dieses, die dritte setzt auf BYOD. Ein Trend zur dritten Gruppe hin ist indes offensichtlich. The Economist erwähnte sinnbildlich das Beispiel Accenture, wo mehr als zwei Drittel der Mitarbeiter die heute 85 000 im geschäftlichen Einsatz stehenden Smartphones und Tablets selbst mitbringen. Noch vor zwei Jahren waren erst 30 000 im Einsatz, die Mehrheit davon vom Unternehmen gestellt.

Cyberkriminelle riechen Lunte

Für Cyberkriminelle steigt der Anreiz, die kleinen Alleskönner ins Visier zu nehmen. In einem Anfang Oktober publizierten Report des IBM-X-Force-Sicherheitsteams prognostizierte der Multi, dass sich die Zahl der Schadprogramme für mobile Endgeräte in diesem Jahr insgesamt verdopple. Das verwundert Sprenger nicht: «Je mehr auf diesen Geräten zu holen ist, desto eher werden sie zum Angriffsziel. Insbesondere die zunehmende Zahl von Smartphones mit eingebauten NFC-Chips, die das Bezahlen mit dem Gerät ermöglichen, dürften für Angreifer immer lukrativer werden.»

Zu denken gibt auch der teils leichtsinnige Umgang mit den mobilen Geräten. Der Sicherheitslösungsanbieter Symantec bestätigte vor einigen Wochen im Cybercrime Report genau dies. Demnach unternehmen nur wenige private Smartphone-Nutzer trotz steigender mobiler Internetkriminalität und der damit verbundenen Befürchtungen effektiv etwas gegen die neuen Gefahren. Nur knapp 13 Prozent haben laut der Erhebung eine App installiert, die bei Verlust des Handys personenbezogene Daten löscht. Zudem verwenden gerade mal 15 Prozent eine App zur Überprüfung der Sicherheit von Dateien und Websites. Insgesamt 16 Prozent haben laut Symantec die neuesten Schutzfunktionen für mobile Sicherheit installiert.

Letzteres könnte sich allerdings bald ändern. «Es ist eine Frage der Zeit, bis – wie bei PCs – ein Mechanismus mit Antivirenprogrammen sowie dem Updatemechanismus üblich sein wird», prognostiziert Sidler. Jedoch werde dies nicht bei allen Plattformen gleich schnell gehen, ergänzt Sprenger. Bedürfnisgetrieben werde es etwa bei den «offenen» Android-Systemen schneller gehen als zum Beispiel beim iPhone.

Was taugt Mobile Device Management?

Ein probates Mittel, um die unterschiedlichen Sicherheitsstandards der Plattformen unter einen Hut zu bringen, sind die eingangs von Sidler ins Gespräch gebrachten Mobile-Device-Management-Lösungen. Mit so einer zentral verwaltbaren IT-Sicherheits-Suite, die Schutz vor Bedrohungen und Datenverlusten bietet, können sich Unternehmen vor den heutigen Bedrohungen schützen und Compliance-Anforderungen nachkommen, die neben Verschlüsselung auch Data Leakage Prevention (DLP) verlangen.

So ermöglichen die von Swisscom angebotenen Device-Management-Lösungen die sichere Einbindung aller im Unternehmen eingesetzten Smartphones und Tablets ins Unternehmensnetzwerk und das Over-the-Air-Management. Der Kunde könne dabei auf jedes einzelne Gerät zugreifen und beispielsweise Neukonfigurationen vornehmen, Geräte identifizieren, freigeben oder sperren. Ebenso lassen sich Applikationen und Software-Updates ohne grossen Aufwand auf den gesamten Gerätepool verteilen.

Etwas weniger begeistert von Mobile-Device-Management-Lösungen ist Sprenger. «Solche Lösungen kapseln den Businessteil vollständig vom privaten Bereich ab. Wir sind der Ansicht, dass man die grunsätzlichen Funktionalitäten und Interaktionsparadigmen des Geräts nicht zu stark einschränken sollte.» Für die Adnovum-Spezialisten ist klar: «Die Security muss – aus Sicht des Benutzers – weiter in den Hintergrund rücken, der Nutzer sollte davon nichts mitbekommen. Im Moment ist die Security zu sichtbar, und der Nutzer muss sich noch zu viele unnötige Gedanken darüber machen.» Zusätzlich sollen Konzepte verfolgt werden, die es erlauben, kritische Daten nicht mehr direkt auf dem Smartphone speichern zu müssen, sondern nur noch zur Ansicht auf demselben zur Verfügung zu stellen.

Ob neben den Digital Natives, technikaffinen CEOs und weiteren Mobile-Device-Begeisterten auch die CIOs dem Einsatz der kleinen Alleskönner im Geschäftsalltag dereinst in corpore positiv gegenüberstehen werden, bleibt nach heutigem Kenntnisstand offen. Solange könnten, angesichts der Risiken, getreu den Warnungen auf den Zigarettenschachteln, auch die Smartphones mit folgendem Hinweis versehen werden: «Die unsachgemässe Nutzung kann Ihrem Arbeitgeber erheblichen Schaden zufügen.» <

10 TIPPS ZUR MOBILEN SICHERHEIT

Am Mediengespräch über Mobile Device Management Anfang Juni empfahl Swisscom folgende zehn Punkte zur Sicherheit von mobilen Geräten im Auge zu behalten:

Aus Anwendersicht:

1. Das Gerät mit einem Passwort und einem SIM-PIN schützen. Das erschwert den Zugriff.
2. Den automatischen Zugriffsschutz, der das Gerät bei Nichtgebrauch sperrt, aktivieren.
3. Wenn Daten per Bluetooth, Infrarot oder USB übertragen werden, nach Gebrauch immer die Schnittstelle ausschalten.
4. Ein Virenschutzprogramm auch auf dem Handy installieren.
5. Die Daten durch ein regelmässiges Back-up sichern.

Aus Architektur- und Netzwerksicht:

1. Definition der businesskritischen Anforderungen und bewusste Auswahl der mobilen Geräte und der Ökosysteme.
2. Sicherer Einsatz von Business-Apps (Security Auditing und Klassifizierung der Daten).
3. Einsatz einer Device-Management-Lösung.
4. Sichere Geräteauthentisierung und sichere Benutzerauthentisierung (MobileID).
5. Definition der erlaubten Transportmechanismen (Public versus Corporate Network Access) und Netzzugänge.