MOBILER SICHERHEITS-HORROR

Unternehmenskommunikation ist ohne Notebooks, Netbooks, Smartphones und Tablets kaum mehr vorstellbar. *Aber die IT-Chefs raufen sich die Haare:* Die Flut an mobilen Devices reißt immer neue Sicherheitslücken auf. Und Abhilfe ist nicht leicht zu finden.

FOTO: PHOTOS.COM

Von Heinz van Saanen

Für breite Bevölkerungskreise ist IT-Security und Datenschutz ein Thema, das ungefähr so spannend ist wie eingeschlafene Füße. Das glauben Europas politischen Eliten wahrscheinlich heute noch, auch wenn sie durch jüngste Umfrage- und Wahlerfolge der »Piraten« leicht verunsichert sind. Dabei muss man kein bunter Pirat sein, um dem grassierenden Überwachungswahn und der Datensammelwut auch negative Seiten abzugewinnen. Vor bald zehn Jahren war der deutsche Industrieadel über den US-Homeland-Security-Act bestürzt – erzkonservative und höchst distinguierte Herren, die ohne Zweireiher, blütenweißes Hemd und Krawatte wahrscheinlich nicht einmal ins Bett gehen. Ihre handfeste Sorge: Seit damals sammelt die US-Behörde etwa auch Lieferscheine und Frachtpapiere in den Häfen und bekommt so ein lückenloses Bild über die US-Aktivitäten der deutschen Industrie frei Haus geliefert. Das nährte den Verdacht, dass die USA in Wirklichkeit weniger an Security als eher an handfester Industriespionage interessiert sei. Ein Verdacht, der heute reihum gereicht wird. Peking spioniert in Washington und vice versa – und alle spionieren in Europa. Der Glaube, dass IT-Hochsicherheitsbastionen unknackbar sind, wurde spätestens letztes Jahr erschüttert. Spektakuläre Einbrüche bei Kreditkartengesellschaften, Telcos, in Firmendatenbanken, der US-Börse Nasdaq und selbst bei Security-Unternehmen und Zertifizierungsstellen zeigten ein düsteres Bild.

Es dürfte wohl auch nur eine Frage der Zeit sein, bis die ersten via Vorratsdatenspeicherung gesammelten Daten über EU-Bürger in dunklen Kanälen landen. Der Fantasie scheinen bei möglichen Einfallstoren kaum Grenzen gesetzt. Wer denkt schon an »dumme« Drucker? Aber erst Ende letzten Jahres bestätigte HP eine potenzielle Schwachstelle für ältere Laserjets. Aber auch Konkurrenzprodukte von Canon und Co zeigen sich für Angriffe auf das Firmennetz immer wieder als verwundbar.

Ein russischer »Angriff« auf Wasserpumpen löste im Dezember in den USA Terroralarm aus. Der Vorfall entpuppte sich zwar schnell als normaler Fernwartungszugriff, zeigt aber, wohin die Sicherheitsreise geht. Scheinbar ist kein Angriff mehr undenkbar. Erstaunlich wenig öffentliche Beachtung findet bislang der boomende Sektor Mobility. Das Abschöpfen von Gesprächen oder

Daten von privaten Handy-Usern dürfte für professionelle Datendiebe vergleichsweise wenig interessant und lukrativ sein. Aber die profane Handynutzung ist ohnehin out. Im Trend liegen alle Arten von Smartphones, Tablets und Konsorten, die auch zunehmend in den IT-Firmennetzen Verwendung finden.

›› Neue Technik – neue Angriffsziele ‹‹

Durch die Einbindung in Firmennetze werden die mobilen Plattformen aber zum lohnenden Ziel – und öffnen für Cracker und böse Buben ein wahres Wunderland an neuen Möglichkeiten. Dafür sorgen gleich mehrere Faktoren. An erster Stelle steht die Verbreitung der neuen Technologien. Schon seit einer Ewigkeit geistert der »Mobile Worker« durch die Untersuchungen der internationalen Marktforscher. Aber jetzt manifestiert er sich so sicher wie unaufhaltsam. Analysten wie Vanson Bourne oder IDC kommen zwar zu leicht unterschiedlichen Befunden, nähern sich im Tenor aber an. In den nächsten zwei, drei Jahren dürfte rund die Hälfte der über 200 Millionen Beschäftigten Westeuropas mehr oder weniger der Kategorie des »mobilen Arbeiters« zuzuordnen sein. Auch Österreich, ohnehin ein klassisches Mobilfunkland mit hart umkämpften Märkten, bleibt nicht abgekoppelt. Zu diesem Schluss kommt die WKO-Fachgruppe UBIT, die jüngst 221 heimische IT-Entscheider zu »Trends und Budgets« befragte (siehe Kasten). Das Fazit der von der WKO in Auftrag gegebenen LSZ Consulting Studie: »Das Management muss Mobile Computing als Trend akzeptieren – und die notwendigen Anpassungen der betrieblichen IT vornehmen«, sagt Robert Bodenstein, Obmann der UBIT Wien. LSZ-Studienautor Alexander Loisel ergänzt: »Auch im Bereich ERP, also Enterprise Resource Planning, gewinnt die Mobilität an Bedeutung. Immer mehr Anbieter setzen auf webbasierte Produkte, um auch unternehmensextern Zugriff auf die komplexen Systeme ermöglichen zu können. Dies bedeutet einen signifikanten Zeit- und damit Kostenvorteil.« Risikofreudiger als bei Cloud-Anwendungen (siehe Kasten) sind Unternehmen im Umgang mit BYOD. Das neue Modewort steht für »bring your own device« und öffnet den Mitarbeitern die Möglichkeit, private Mobilfunk-Hardware auch beruflich zu nutzen. BYOD erlauben – Tendenz steigend – lediglich 16 Prozent der heimischen Unternehmer.

»DAS MANAGEMENT *muss Mobile Computing als Trend akzeptieren und die notwendigen Anpassungen der betrieblichen IT vornehmen«, sagt Robert Bodenstein, Obmann der WKO-Fachgruppe UBIT Wien.*

Im Vergleich sind heimischen IT-Chefs hier also zurückhaltender als ihre internationalen Kollegen, wie ein Vergleich mit aktuellen Studien von Marktforschern wie etwa Forrester nahelegt. Die Zurückhaltung hat rationale Gründe. Wer BYOD uneingeschränkt erlaubt, öffnet die Schleusen für neue sicherheitsrelevante Einfallstore. Die IT-Abteilungen dürfen dann nämlich einen Flohzirkus von Hardware, Betriebssystemen oder Geräteklassen – alles vielleicht noch hübsch permutiert über Soft- und Hardwareversionen – integrieren, verwalten und abdichten. Auch wenn, um nur ein paar der echten Big Player zu nennen, Apple, Android oder Windows Mobile den Löwenanteil der Märkte abdecken, identifiziert der einschlägige Gartner-Report 2011 Dutzende von Anbietern, die ebenfalls eine wichtige Rolle spielen. Speziell für Mittelständler ohne hauseigene Hardware- und Software-Experten dürfte eine sicherheitstechnisch wasserdichte Integration aller mobilen Devices daher völlig illusorisch sein. Das legt auch eine aktuelle Untersuchung des deutschen Bundeswirtschaftsministeriums nahe, nach der ein Fünftel der deutschen KMU bei Mobilgeräten ⇨

MOBILE COMPUTING IST GELANDET

›› Schon seit einer gefühlten Ewigkeit geistert der »Mobile Worker« durch die Analysen der internationalen Marktforscher. Jetzt manifestiert er sich – auch in Österreich – unaufhaltsam. Zu diesem Schluss kommt die WKO-Fachgruppe UBIT, die erst jüngst 221 heimische IT-Entscheider zu »Trends und Budgets« befragte. Fast schon die Hälfte der CIOs gab an, dass ihr Unternehmen Firmenanwendungen auf privaten Endgeräten bereits jetzt unterstütze. Mobilität und »Apps« werden auch heuer an Bedeutung zulegen und die Beschaffungslandschaft ändern. Heuer werden Smartphones erstmals Notebooks als meist genutztes Endgerät ablösen. Auch Tablet-PCs liegen in der Nutzung fast schon gleichauf mit klassischen Notebooks. Schwerpunkt der mobilen Nutzung ist E-Mail, gefolgt von ERP-Anwendungen. ERP erlebt im Zusammenhang mit Mobile Computing einen x-ten Frühling – und wird das Top Thema 2012. Immer wichtiger wird der externe und webbasierte Zugriff auf die IT. Mit echten Cloud-Lösungen können sich jedoch zwei Drittel der IT-Mananger noch nicht anfreunden.

➪ sogar auf Passwörter verzichtet oder Smartphones nur zu knapp zehn Prozent mit einer Firewall abgesichert sind. Für Österreich dürften die Zahlen nicht viel anders aussehen.

»DAS PROBLEM *mit mobilen Devices ist nicht nur die Technik. Vor den Endgeräten sitzt immer ein Mensch«, so Christian Reiser, Sicherheitsexperte der Erste Group.*

»» Chaotischer Sicherheitsmarkt ««

»Problem erkannt – Problem gebannt« ist eine Weisheit, die ausgerechnet beim Markt für mobile Security nicht so recht greift. Schon der Hardwaremarkt ist mehr als turbulent. Heute dominieren Geräteklassen, die vor ein paar Jahren noch nicht einmal bekannt waren. Um 2000 herum wurde ein Handy noch knapp zwei Jahre benützt, aktuelle Smartphones kommen beispielsweise gerade einmal noch auf einen »Lebenszyklus« von durchschnittlich 11,5 Monaten. Noch chaotischer und dynamischer als bei mobiler Hardware und Betriebssystem stellt sich der Markt für mobile Sicherheitslösungen dar. Wer seine mobile IT-Umgebung absichern will, muss sich mit »Mobile Device Management« beschäftigen (siehe Kasten). Aber ausgerechnet der MDM-Markt ist höchst unübersichtlich. Selbst Marktleader wie Good Technology, Mobilelron, Sybase oder Airwatch dürften landläufig eher nur Spezialisten bekannt sein. Der junge Markt ist höchst turbulent. Wer sicherheitstechnisch nicht den Überblick verlieren will, muss auf Reduktion setzen. Weniger mobile Vielfalt bringt mehr Sicherheit, weniger Kosten und einfachere IT-Integration. Aber vor allem: einen kleineren Kreis von etablierten Anbietern. Unternehmen sollten daher auch namhafte »MDM-Outsider« in Betracht ziehen, die ihre Kunden ebenfalls mit einschlägigen Lösungen versorgen könnten (siehe Kasten).

Diese großen Namen sind vielleicht weniger »trendy« und »hip« als die zahlreichen kleinen und coolen Start-ups, dafür gibt es heute schon lokalen Support , und – für Unternehmen als Planungs- und Sicherheitsfaktor nicht unerheblich – morgen mit hoher Wahrscheinlichkeit auch noch die Anbieter selbst. Nicht ohne Grund analysieren etwa die Marktforscher von Gartner in ihrem MDM-Report 2011 nicht nur die üblichen Stärken und Schwächen der Anbieter, sondern führen eigens eine Rubrik »Vorsicht« mit an. Abseits von möglicher technischer Brillanz finden sich dort nüchterne Einschätzungen wie »derzeit nur in wenigen Ländern marktrelevant« oder »ungewisse Wachstums- oder Finanzierungsaussichten«. Weitgehend unberechenbar und irrational ist ohnehin der Faktor Mensch. Am sichersten dürfte es sein, ausschließlich altbekannte und bewährte Plattformen wie Windows Phone oder BlackBerry OS einzusetzen. Für diese gibt es Integrations-Knowhow und Support. Aber was ist schon vernünftig? »Das Problem mit mobilen Devices ist nicht nur die Technik. Vor den Endgeräten sitzt immer ein Mensch«, sagt Christian Reiser, Sicherheitsexperte der Erste Group. Besonders problematisch werde es, wenn das Management immer das »gerade geilste Endgerät brauche«. Dann laufen zwar die Manager mit den angesagtesten mobilen Gadgets durch die Gegend – aber mit deren Integration und Sicherheit dürfen die IT-Abteilungen kämpfen. ■

FOTO: PHOTOS.COM

SUCHE NACH DER NADEL IM MOBILE-SECURITY-HEUHAUFEN

»» Der Markt für Sicherheitslösungen im Bereich Mobility ist, gelinde gesagt, unübersichtlich. Dafür sorgen schon Dutzende von Geräteherstellern, Geräteklassen und Betriebssysteme. Wer den mobilen Zoo absichern will, muss sich mit »Mobile Device Management«, kurz MDM, auseinandersetzen. Aber auch der MDM-Markt ist unübersichtlich. Marktforscher Gartner identifiziert rund 60 Anbieter – die meisten dürften nur Spezialisten bekannt sein. In Stein gemeißelt ist ohnehin nur wenig, Übernahmen oder auch Kindesweglegungen sind an der Tagesordnung. HP oder Nokia etwa sind eingestiegen, wieder ausgestiegen und trotzdem irgendwie noch dabei. Klassische Antiviren-Hersteller wie McAfee oder Symantec wiederum drängen in den turbulenten MDM-Markt, besetzen aber derzeit laut Gartner nur Nischen. Lindern lässt sich die Qual der Wahl durch Faustregeln. Die wichtigste: Weniger ist mehr! Wer seine Mitarbeiter auf BlackBerry oder das »alte« Windows Phone festnagelt, findet ein breiteres Spektrum an ausgereiften Lösungen. Wer schon SAP im Einsatz hat, sollte sich die Lösungen der SAP-MDM-Tochter Sybase ansehen. Wer statt Start-ups lieber auf bekannte Namen und lokalen Support setzt, sollte vielleicht auch bei IBM, HP, Microsoft, BMC oder CA nachfragen. Diese zählen zwar nicht zum Kern der MDM-Anbieter, bieten aber ihren Firmenkunden entsprechende Lösungen, sofern die IT-Landschaft »passt«. Ähnliches gilt für Integratoren wie T-Systems, Hardware-Hersteller wie Fujitsu, Motorola/Google oder selbst Provider wie T-Mobile. Skepsis ist bei Anbietern von »eierlegenden Wollmilchsäuen« angebracht. Wer schon heute Dutzende mobile Plattformen »schmerzfrei« und sicher auf ein Dutzend ERP-Systeme integriert, ist der Aktientipp von morgen – oder der Scharlatan von heute.