»OBSERVER«
A-1020 Wien, Lessinggasse 21
www.observer.at, E-Mail: info@observer.at
Fon: +43 1 213 22 *0, Fax: +43 1 213 22 *300
Auflage: 12040 Auftrag Nr: 2391
Verlagstel.: 01/5221414 Clip Nr: 8084525
Größe: 94,83% SB: Up to Eleven
Extradienst
Wien, November 2013 - Nr. 10

Innere Sicherheit

Ein aktueller Trend in den Unternehmen lautet „Bring your own device“: Mitarbeiter nutzen ihre persönlichen Handys oder Tablets gleichzeitig privat sowie beruflich. Was eine Herausforderung für den Schutz heikler Daten bedeutet.

Von Christian Prenger

Privatsphäre, Sicherheit, Datenschutz: „Bring your own device“ erweist sich als anspruchsvolle Materie

Coole Kürzel gehören fast schon zur Folklore der IT-Industrie. ECM, BPM, ERP und mehr zählen zur verbalen Grundausstattung von Experten. Jetzt macht eine neue Kreation die Runde: BYOD oder „Bring your own device“ beschäftigt gerade die Strategen in vielen Unternehmen.

Hinter dieser Aufforderung verbirgt sich eine trendige Entwicklung: Seit iPhone, iPad und Co. zu Drehscheiben des täglichen Lebens avanciert sind, wollen viele Mitarbeiter im Job nicht auf ihre persönlichen Endgeräte verzichten, die ohnehin überall dabei sind. Immer öfter sind Manager mit der Tatsache konfrontiert, dass ihr Personal Hardware gleichzeitig beruflich und privat nutzen möchte.

Was nicht zuletzt Chefs im Mittelstand gelegen kommt – so lässt sich ein schwaches Budget für elektronische Investitionen schonen, da Anschaffungskosten für teure, professionelle Geräte entfallen. Die Rasanz der digitalen Welt ist ebenfalls optimaler zu bewältigen: Neue Modelle kommen immer schneller auf den Markt und sind selten billig. Was kann besseres passieren, als dass Techno-Freaks aktuelle Überflieger auf eigene Kosten erwerben.

Sinkende Wartungskosten

Die Wartungskosten sinken gleichermaßen, nicht nur, weil Fachkräfte persönliche Elektrobegleiter meist besser behandeln als das klapprige Handy mit Dinosaurier-Touch, das der Betrieb zur Verfügung stellt. Für kleine Probleme am Endgerät muss nicht gleich ein interner, technischer Helfer anrücken oder der Support Überstunden einlegen – da weiß der Besitzer selbst, wie erste Hilfe zu leisten ist.

„Bei BYOD wird das Management von Endgeräten auf den Mitarbeiter übertragen. Dies kommt auch KMUs entgegen, da deren IT-Abteilungen häufig unterbesetzt sind und eine zeitaufwendige Aufgabe nicht haften bleibt“, weiß Peter Wirnsperger, Experte des Beratungsunternehmens Deloitte.

Der Trend hinterlässt also offenbar positive Spuren, was die Geldbörse betrifft. „Durch dieses vereinfachte Management ergeben sich für die IT-Einsparungen von bis zu 30 Prozent“, verkündet Margarete Schramböck, Geschäftsführerin des Lösungsanbieters NextiraOne.

Achim Kaspar, General Manager von Netzwerkspezialist Cisco Austria, ortet ebenso Finanzpotenzial: „Gemäß der Funktion des Mitarbeiters und damit verbundenen Anforderungen sind die Geschäftsvorteile unterschiedlich. Abhängig von der Position können mit dieser Strategie Einsparungen von je 250 bis 1000 Euro realisiert werden.“

Kenner verweisen zusätzlich auf Umwegrentabilität. Wenn Kollegen mit ihren eigenen coolen Devices auch arbeiten dürfen und am Schreibtisch kein Gerätezoo nervt, wächst die

Mobileiron

»OBSERVER«
A-1020 Wien, Lessinggasse 21
www.observer.at, E-Mail: info@observer.at
Fon: +43 1 213 22 *0, Fax: +43 1 213 22 *300
Auflage: 12040 Auftrag Nr: 2391
Verlagstel.: 01/5221414 Clip Nr: 8084525
Größe: 99,17% SB: Up to Eleven
Extradienst
Wien, November 2013 - Nr. 10

Motivation, lautet das Credo. Was Kritiker fundamental bezweifeln: nur wegen eines Smartphones werden Fachkräfte kaum mehr oder weniger arbeiten.

Produktives Personal

Eine Studie der Marktforscher von Ipsos im Auftrag des IT-Spezialisten Citrix zeigt eine Richtung auf: In Deutschland verzeichnet mehr als jedes zweite von fünf Unternehmen mit BYOD einen Produktivitätszuwachs von über 20 Prozent.
Doch selbst solche Perspektiven können keineswegs verdecken, dass jene Entwicklung über Schattenseiten verfügt: Viele IT-Manager zeigen Skepsis hinsichtlich der Datensicherheit. Mobile Geräte erfreuen sich ohnehin heute steigender Popularität bei Industriespionen und Hackern – wenn dann jede Menge Betriebssysteme und Modelle im Einsatz sind, droht organisatorisches Chaos.
Einheitliche Kontrolle und externe Abschirmung mutiert so nur allzu schnell zum Stresstest. Die Szenarien treiben so manchen Hütern der Netzwerke Schweiß auf die Stirne: Dann loggt sich der Aussendienstmitarbeiter im Kaffeehaus zwischen Sandwich und Prosecco schnell einmal in das kostenlose, drahtlose Internet des Gastronomen ein, um seine Mails in der Firma abzurufen und sich über die letzten Firmeninterna zu informieren – wo jedoch niemand sagen kann, ob diese Verbindung richtig geschützt ist. Schon besteht die Gefahr, dass heikle Daten am Gerät ein offenes Buch darstellen.
Was gleichfalls zeigt, dass es sich bei BYOD nicht um eine harmlose Geste für Digital Natives handelt, sondern um eine komplexe Materie, die effiziente Reaktionen erfordert. Sonst kostet die Sache vielleicht mehr als sie bringt. Denn etwa über Security-Schwachstellen ausspionierte und dann eiskalt kopierte Innovationen, die noch nicht zum Patent angemeldet sind, könnten plötzlich in ganz andere Hände gelangen – mit möglicherweise unabsehbaren Folgen.

Betriebliche Turbulenzen

Aber auch innere Turbulenzen sind keineswegs ausgeschlossen. Laut einer Studie von Mobileiron herrschen Auffassungsunterschiede zwischen Angestellten und Arbeitgebern, wenn es darum geht, was auf einem mobilen Gerät privat ist und was nicht. Nach der Analyse jenes Lösungsanbieters für Mobile Device-Management war für fast Hälfte der Befragten

»OBSERVER«
A-1020 Wien, Lessinggasse 21
www.observer.at, E-Mail: info@observer.at
Fon: +43 1 213 22 *0, Fax: +43 1 213 22 *300
Auflage: 12040 Auftrag Nr: 2391
Verlagstel.: 01/5221414 Clip Nr: 8084525
Größe: 95,13% SB: Up to Eleven
Extradienst
Wien, November 2013 - Nr. 10

Peter Wirnsperger, Deloitte: BYOD entlastet auch KMUs von einer zeitaufwendigen Aufgabe

Kerstin Rucker, Up to Eleven: Bei Choose your own Device wählen Mitarbeiter ihr bevorzugtes Modell

Achim Kaspar, Cisco Austria: Die Absicherung muss einen hohen Stellenwert einnehmen

klar, dass ihre Chefs keinerlei Informationen auf ihren Endgeräten sehen können, während sich 15 Prozent nicht sicher waren.
Nur 28 Prozent denken, dass ihr Unternehmen ihre beruflichen E-Mails sowie Anlagen sehen kann, während lediglich 22 Prozent glauben, dass ihre beruflichen Kontakte für das entsprechende Unternehmen sichtbar sind. In der Realität läuft die Sache aber anders: Wenn Geräte zum Erhalt von E-Mails des Unternehmens genutzt werden, können Arbeitgeber berufliche Post sowie Anhänge genauso einfach ansehen wie auf einem PC. Hier besteht eine große Kluft zwischen Erwartung und Realität.
Die Materie erweist sich also generell als überaus anspruchsvoll – was so manchen Betrieb auch abhalten dürfte, jenes Konzept einzuführen. Wenn es soweit ist, fordern Berater eine bewusste Strategie statt Zuschauen.
Hier besteht jedoch ein klares Defizit in Österreich. Schramböck: „Viele Unternehmen besitzen immer noch kein Konzept für sichere Einbindung von mobilen Devices in ihr Netzwerk. Nur 32 Prozent der Betriebe verfolgen hier einen klaren Plan. Die Ursache ein mangelndes Risikobewusstsein bei Verantwortlichen."

Ignorierte Verbote

Vielfach ist aber sehr wohl Einsicht vorhanden, doch fehlt wegen geringer Erfahrung mit dem gerade trendigen Phänomen das Know-how. Radikale Ansätze wie das strikte Verbot der Doppel-Nutzung beenden zwar alle Diskussionen über Pro und Kontra, gehen aber an der Lebensrealität und an Sparmöglichkeiten vorbei. Pikantes Detail: Insider erzählen, dass manche Mitarbeiter ein „Njet" ohnehin ignorieren – bis den Chefs der Kragen platzt.
Eine verträglichere Option bilden exakte Vorgaben, die etwa die Verwendung sicherheitstechnisch bedenklicher Apps für die Freizeit genauso einschränken wie den Gebrauch von Cloud-Diensten, weil hier Daten häufig auf Servern liegen, deren Standorte aber unbekannt sind.
Was eine Mischung aus strategischem Bewusstsein für die Situation inklusive klarer Konzepte voraussetzt. Kaspar: „Die Absicherung muss einen hohen Stellenwert einnehmen. Es geht um ganzheitliche Lösungen, die netzwerkzentriert ausgerichtet sind. Klare Regeln und Richtlinien zur Nutzung privater Geräte sind notwendig."
Mit umfassenden Konzepten und effizienter Technologie lässt sich BYOD also zumindest in den Griff bekommen. „Systeme wie die Virtualisierung oder Verschlüsselung erlauben es, solche Geräte schnell und einfach in die Infrastruktur von Firmen zu integrieren. Selbst bei Diebstahl oder Verlust gibt es sehr gute Systeme zur Ortung oder Löschung von Geräten aus der Ferne. Die Möglichkeiten sind unbegrenzt, sollten aber durchdacht werden", erklärt Dominik Unger, IT-Leiter im Mucha Verlag.

Mehr Systeme

Die Industrie reagiert auf allfällige Bedürfnisse mit einer wachsenden

Deloitte, Cisco Austria, Up to Eleven , NextiraOne

»OBSERVER«
A-1020 Wien, Lessinggasse 21
www.observer.at, E-Mail: info@observer.at
Fon: +43 1 213 22 *0, Fax: +43 1 213 22 *300
Auflage: 12040 Auftrag Nr: 2391
Verlagstel.: 01/5221414 Clip Nr: 8084525
Größe: 100% SB: Up to Eleven
Extradienst
Wien, November 2013 - Nr. 10

Menge an Systemen. Softwarehersteller United Planet etwa offeriert eine Applikation namens „Bring your own Device", mit der Mitarbeiter alle Endgeräte erfassen, die sie beruflich einsetzen möchten. Mittels Angaben zu Hersteller, Modell, Betriebssystem und Version wird sofort eine Sicherheitseinstufung angezeigt.

Wunschliste

Nach der Wahl gewünschter Dienste wie den Zugriff auf das Unternehmensportal und E-Mails erhält der User ein Dokument zu Security sowie Datenschutz angezeigt, das er lesen und bestätigen muss. Im Falle eines Verlustes kann der Betreffende das Gerät sogar aus der Ferne vom Firmennetz nehmen und möglichen Datenklau verhindern.

Margarete Schramböck, Nextira-One: Einsparungen für die IT von bis zu 30 Prozent

Künftig könnte noch eine Alternative an Kraft gewinnen, die Sicherheit plus Vorteile der Mitbringoption verspricht: CYOD (Choose your own Device), wie es das Grazer Unternehmen Up to Eleven praktiziert. Sprecherin Kerstin Rucker: „Mitarbeiter wählen aus einer stets aktuellen Liste ihr bevorzugtes Modell. Das Gerät wird ebenso für den privaten Gebrauch gestellt. So arbeitet jeder weiter mit seiner bevorzugten Hardware." Der Vorteil: Die Mitarbeiter müssen sich nicht erst in ein neues Gerät einarbeiten und können ihrem gewohnten Arbeitsablauf via Mobile weiter nachgehen. Das Unternehmen kann davon ausgehen, dass die Sicherheit seiner internen Netzwerke gewährleistet bleibt. Nebeneffekt: Möglicherweise bringt das Modell generell auch einigen Managern weniger Stress.