TREND ZUM SELBST-VERSORGER

Bring Your Own Device

Bring Your Own Device macht Unternehmen effizient, Mitarbeiter glücklich – und CIOs grosse Sorgen. Denn die Integration der unterschiedlichen Geräte in bestehende Infrastukturen birgt Risiken. Die Unternehmen müssen eigene Wege finden, damit umzugehen. → VON RETO VOGT

Alpfahrt mit Sack und Pack an der Viehschau Wald-Rehetobel, Kanton Appenzell Ausserrhoden

BILD: KEYSTONE/REGINA KUEHNE

Die Consumerization der IT zwingt CIOs zum Umdenken. Im Privatleben von trendigen Smartphones, Tablets oder Ultrabooks verwöhnt, wollen moderne Wissensarbeiter auch im Büro nichts mehr von verstaubten Computern wissen und ihre geliebten mobilen Devices innerhalb der Firmeninfrastruktur nutzen. Bis vor Kurzem konnten die IT-Leiter die Türe noch verbarrikadieren, aber in Zukunft kommen sie nicht mehr umhin, ihren Mitarbeitern diesen Wunsch zu erfüllen. Zu gross ist die Gefahr, dass qualifizierte Fachkräfte ohne mobilen Zugriff unproduktiver sind oder zur aufgeschlosseneren Konkurrenz wechseln.

Zu lösen gibt es dabei hauptsächlich drei grosse Probleme: Zum einen sind Android-Geräte aufgrund ihres offenen Betriebssystems anfällig für Schädlinge. Bei iPads und iPhones macht aufgrund der geschlossenen Umgebung die Integration in die bestehende Infrastruktur Probleme. Zudem sehen sich die CIOs einer Flut neuer Gerätetypen gegenüber, um die sie sich künftig kümmern müssen. Auf den IT-Verantwortlichen kommen also viele Wünsche, viele Betriebssysteme und viele verschiedene Geräte zu, die er möglichst nahtlos in die Infrastruktur des Unternehmens einbinden muss.

KONTROLLIERTE FREIHEIT

Berechtigte Gründe für das Stirnrunzeln bei den CIOs gibt es trotz der stets wachsenden Bedürfnisse zumindest punkto Smartphone- und Tablet-Handling jedoch keine mehr. Längst gibt es dafür geeignete Software. Swisscom bietet ihren Kunden zum Beispiel eine angepasste Lösung von MobileIron an, über die alle wichtigen mobilen Betriebssysteme wie Android, BlackBerry, iOS sowie Windows Phone in die Firmenumgebung integriert werden können. Die Software übernimmt die zentrale Geräteverwaltung und die Kostenkontrolle für Gespräche und Datenverkehr. Zudem kann der CIO einsehen, welche Apps auf den Geräten installiert sind, welche Einstellungen der Mitarbeiter vorgenommen hat und ob etwa ein unerlaubter «Jailbreak» durchgeführt wurde. Diese Lösung kommt unter anderem bei der Flughafen Zürich AG zum Einsatz. Walter Hofmann, Head of IT Operations und Stellvertretender CIO, erklärt, wie: «Wir integrieren sämtliche Smartphones über das Mobile-Device-Management-System von MobileIron.» Nicht registrierte Geräte bleiben aus Sicherheitsgründen gesperrt ebenso wie manche Funktionen: «Wir lassen ausserdem nur wichtige Funktionen wie den E-Mail-Abruf und die Synchronisation von Aufgaben, Kalender und Kontakten zu», erläutert Hofmann, der den IT-Basisbetrieb am Flughafen verantwortet. Dadurch kann die Geräteauswahl den Mitarbeitenden überlassen werden. Zwar sind die geschäftlich finanzierten Mobiltelefone bei der Flughafen Zürich AG auf Apple und Windows beschränkt, aber mitbringen darf die Belegschaft auch Android-Smartphones.

Bei der Stadt Zürich dürfen die Mitarbeitenden aus einem begrenzteren, vorgegebenen Geräteangebot wählen. In der Stadtverwaltung werden die Betriebssysteme Android und iOS unterstützt, allerdings ist bei Ersterem die Auswahl auf drei Smartphones eingeschränkt, wie Werner Kipfer, GL-Mitglied bei Organisation und Informatik (OIZ), erläutert. Zum Synchroni- →

«Die Geräte stehen denen zur Verfügung, die sie brauchen. Das hat nichts mit der Hierarchiestufe zu tun»

Damir Bogdan, CIO Raiffeisen Gruppe

sieren nutzt die Stadtverwaltung einen selbst entwickelten AirSync-Service. Dieser unterstützt lediglich den Abgleich von E-Mail, Kalender und Kontakten, beim iPhone können zusätzlich noch Aufgaben synchronisiert werden. Über ein Zertifikat lassen sich sämtliche unterstützten Geräte und deren Benutzer identifizieren und vor unberechtigtem Zugriff schützen, so Kipfer.

SCHNELL UND UNKOMPLIZIERT

Einen wesentlich unkomplizierteren Weg wählt der Schweizer Kaffeedistributor Mocoffee. «Die ganze Verkaufsmannschaft ist mit iPads, iPhones und Notebooks ausgestattet», berichtet CEO Pascal Schlittler. Eine spezifische Verwaltungs-Software kommt dabei aufgrund der geringen Firmengrösse von 40 Mitarbeitern nicht zum Einsatz. Das Unternehmen speichert nach eigener Aussage praktisch zu Hundert Prozent in der Cloud. «Neue Geräte können innerhalb von Minuten mit dem firmeneigenen Google-Account synchronisiert werden. Bei der Benutzeridentifizierung setzt Mocofee ebenfalls eine Google-Lösung namens «Authenticator» ein. Bei Zugriffen erhalten die jeweiligen Anwender, ähnlich wie beim E-Banking, einen Zahlencode per SMS zugeschickt. Zusätzlich lassen sich über das Verwaltungsportal unter anderem zeitlich begrenzte Passwörter und eine Mindestlänge definieren.

Bei Geräteverlusten kann Mocoffee laut Schlittler die iPhones über den iFinder orten und sämtliche Daten löschen. Der E-Mail-Zugriff lässt sich über die Google-Administration entfernen. Zudem würden die Zugriffe auf interne Webseiten per Google Analytics geprüft. So könne man Fremdzugriffe relativ schnell identifizieren. «Wir schützen unsere Informationen in einem für unsere Verhältnisse sinnvollen Rahmen. Schliesslich sind wir keine Bank», so Schlittler.

HOCHSICHERHEITSTRAKT

Ganz anders sieht es bei der Bankengruppe Raiffeisen aus. Den Schieberegler zwischen den beiden Extremen «hochflexibel» und «hochsicher» stellt deren CIO Damir Bogdan recht restriktiv ein, denn die hochsensiblen Bankdaten müssen vor Unbefugten geschützt werden. «Wir geben deshalb die Hardware und das Betriebssystem vor», sagt Bogdan. Unterstützt werden lediglich BlackBerrys und das HTC Desire mit Android. Tablets supportet die Bank nicht aktiv, erlaubt aber den Zugriff aufs Firmennetzwerk via Citrix. Vertrauliche Daten kapselt das Finanzinstitut laut Bogdan in einer verschlüsselten SandBox ab, Citrix-Verbindungen werden über VPN und RSA (ein kryptografisches Verfahren mit zwei Schlüsseln) gesichert. Dagegen verzichtet die Bank darauf, bestimmte Applikationen, Funktionen oder Webseiten für die Smartphones zu sperren.

BRING YOUR OWN IST TATSACHE

Wie auch immer die Unternehmen den Umgang mit den mobilen Devices im Detail regeln, ein Trend ist bei allen zu beobachten: Während es früher üblich war, nur Kaderangestellte mit den neusten Geräten auszurüsten, steht heute die fachliche Funktion im Vordergrund. «Die mobilen Geräte stehen den Mitarbeitern zur Verfügung, die sie auch benötigen. Die Vergabe hat nichts mit der Hierarchiestufe zu tun», sagt Raiffeisens CIO Damir Bogdan. Dasselbe gilt für den Flughafen Zürich: «Ein Smartphone erhält jeder, der telefonisch erreichbar sein muss», so der IT-Verantwortliche Walter Hofmann.

Die Stadtverwaltung Zürich mit ihren rund 25 000 Mitarbeitern regelt dies ähnlich. Deren Mitarbeitende müssen für die geschäftliche Nutzung von Smartphones ein Geschäftsabonnement abschliessen, das die Stadt komplett finanziert. Die Kosten für die Hardware tragen

«Mitarbeiter der Stadt profitieren von vergünstigten Tarifen und können einen Corporate-Mobile-Network-Vertrag abschliessen»

Werner Kipfer, Leiter Applikationen OIZ

«Wir lassen nur wichtige Funktionen wie E-Mail und Synchronisation von Kalender und Kontakten zu»

Walter Hofmann, Head of IT Operations, Flughafen Zürich

die Mitarbeiter nur, wenn sie das Gerät hauptsächlich privat nutzen. «Es besteht zudem die Möglichkeit, von vergünstigten Tarifen zu profitieren und einen Corporate-Mobile-Network-Vertrag (CMN) abzuschliessen», sagt Werner Kipfer. In diesem Fall sei der Arbeitgeber zwar Inhaber des Mobilfunkabos, aber die Rechnung übernähmen jeweils die Mitarbeitenden. Sofern Mitarbeiter der Stadt bereits Geräte besitzen, die mit der Synchronisierungs-Software AirSync-Services kompatibel sind, dürfen auch diese verwendet werden. Nebst Apples iPhone zählt dazu laut Kipfer unter anderem Samsungs Galaxy SII. Auch Flughafenmitarbeiter dürfen nach Auskunft von CIO Walter Hofmann ihre privaten Smartphones und Tablets für geschäftliche Tätigkeiten nutzen.

«Bring Your Own Device» ist heute in allen Branchen hoffähig – nicht nur in Verwaltung und Industrie, sondern auch in Finanzinstituten. «Mitarbeiter, die über die Möglichkeit von Home Office verfügen, nutzen zu Hause ihre persönlichen Geräte», wie Raiffeisen-CIO Damir Bogdan erklärt. Dort gelten die internen Hardware-Vorgaben nicht: «Zwar ist die Funktionalität eingeschränkt, aber grundsätzlich ist jedes mit Microsofts Betriebssystem betriebene Gerät kompatibel – sogar Tablets.»

FAZIT: AUF DIE MITARBEITER HÖREN

Unabhängig von Grösse und Branche sollten CIOs auf die Wünsche der Mitarbeiter hören und diese auch umsetzen. Die Unternehmen profitieren davon mehrfach, wie Flughafen-CIO Walter Hofmann resümiert: «Die Mitarbeitenden erscheinen mit grösserer Motivation am Arbeitsplatz, können sich in ihrer gewohnten, vertrauten Umgebung bewegen, greifen von überall auf ihre Daten zu und sind schneller informiert.» ←