Christian Wege

Bring Your Own Device

Direkt von der Warteschlange vor dem Flagship Store zum Unternehmens-Campus in der Hand der Mitarbeiter. Diesen Weg nehmen zunehmend mehr Smartphones und begründen damit einen Hype, der zur Zeit über viele große Unternehmen und deren Mitarbeiter schwappt: „Bring Your Own Device", abgekürzt BYOD.

BYOD beschreibt den Fall, dass Mitarbeiter ihre Endgeräte in begrenztem Umfang zu geschäftlichen Zwecken nutzen. Insbesondere sind damit mobile Endgeräte wie Smartphones und Tablets gemeint. Die Nutzung reicht vom Synchronisieren der geschäftlichen E-Mails bis zum Zugriff auf Datenbanken mit vertraulichem Inhalt. Außerdem löst die Nutzung privater Endgeräte das Problem, dass auf vielen firmeneigenen Geräten meist nur in begrenztem Umfang private Inhalte wie Musik, Videos, Bücher, etc. erlaubt sind. Private Apps dagegen üblicherweise nicht. Damit ist die Nutzbarkeit dieser Geräte oft in Frage gestellt. Wenn man schon ein Smartphone mit sich rumträgt, dann möchte man doch auch *Whatsapp*, *Twitter*, *Clouds* & *Sheep*, und wie sie alle heißen, nutzen.

Laut CISCO nutzen inzwischen 42 Prozent aller Knowledge Worker weltweit ihre privaten Endgeräte auch in diesem Sinne. Dabei hinken nach dieser Studie manche europäische Staaten wie Frankreich, Deutschland, Russland und Großbritannien hinterher, während Asien und Lateinamerika große Zuwachsraten erleben.

Ganz neu ist die Nutzung von privaten Ressourcen nicht. Beispielsweise, wenn man mit dem geschäftlichen Laptop über den privaten Internetzugang auf das geschäftliche Netzwerk zugreift. Aber durch die massive Verbreitung von mobilen Endgeräten und dem damit aufkeimenden Wunsch, auch damit auf geschäftliche Ressourcen zuzugreifen, entstehen neue Herausforderungen.

Technisches

Der Zugriff der privaten Endgeräte auf die Geschäfts-Ressourcen erfolgt oft über den Internet-Zugang in den Geräten. Diese sind heute meist sowieso mit einer *flat rate* ausgestattet. Sehr schnell kommt aber auch der Zugang über ein schon vorhandenes WLAN im Büro ins Gespräch – um die private *flat rate* zu schonen. Die vordringliche Herausforderung ist aber die Security-Integration der Geräte mitsamt den notwendigen Richtlinien.

Der aktuelle IBM X-Force-Bericht gibt eine Übersicht zu den sicherheitsrelevanten Bausteinen. Unter anderem gehört dazu die Kapselung der geschäftlichen Daten auf dem privaten Endgerät. Hier sind schnell spezialisierte Lösungen entstanden wie Good for Enterprise als Container für Unternehmens-Daten. Ein solcher Container kann eine separate Authentisierung auf dem Endgerät erfordern, bevor der Nutzer auf darin gespeicherten Daten zugreifen kann. Die Versorgung von geschäftlichen Daten (z. B. E-Mail) erfolgt in diesem Fall lediglich in dem Container. Dieser bietet darüber hinaus die Möglichkeiten der Fern-Löschung – beispielsweise für den Fall eines Diebstahls des Geräts (oder Ausscheidens des Mitarbeiters). Ein weiterer sicherheitsrelevanter Baustein ist die Integrität des Betriebssystems. So erleichtert das beliebte Aufheben der Zugriffsbeschränkungen durch den Nutzer (*jail break* oder *rooted*) ein Umgehen der mit dem Container eingeführten Sicherheits-Maßnahmen. Solchen Geräten bleibt daher der Zugriff auf Unternehmensdaten gerne verwehrt. Die Möglichkeiten der Integration in die IT-Infrastruktur des Unternehmens hängen zum einen von den Fähigkeiten der zugelassenen Endgeräte ab. Dabei ist es für die IT-Abteilungen nicht leicht, bei den ständigen Veränderungen im Markt der mobilen Endgeräte am Ball zu bleiben. Zum anderen hängt die Integration von den in der IT-Infrastruktur vorhandenen Diensten ab. Beispielsweise erfolgt beim Einsatz von Desktop-Virtualisierung (wie etwa Citrix) die Verarbeitung vollständig auf den Unternehmens-Servern. Auf dem Endgerät ist hierbei nur die Oberfläche zu sehen und somit ist ein breites Einsatzspektrum möglich. Fehlt ein solcher Dienst hingegen, ist eher eine Beschränkung auf PIM-Funktionalität (E-Mail, Kalender, Adressbuch) üblich. Hier bietet sich dann aber beispielsweise an, eine kombinierte Sicht auf den privaten und geschäftlichen Kalender zu erstellen.

Eine weitere ernst zu nehmende Herausforderung ist, wie Fehler bei der Integration der privaten Endgeräte behoben werden. Der Helpdesk ist auf die geschäftlich bereitgestellten Geräte ausgelegt. Andererseits sind die Mitarbeiter mit der Fehlersuche und Behebung meist überfordert. Dazu kommt, dass es natürlich immer die neuesten Geräte sein müssen. Nach dem Schlangestehen ist vor dem Schlangestehen.

Organisatorisches

Übliche offen vorgetragene Argumente für BYOD sind:

- Mitarbeiter bringen ihre Endgeräte sowieso mit und wollen auch damit auf ihre wichtigsten Firmendaten zugreifen (wie E-Mail, Kalender, Adressbuch).
- Die „*Always-on*-Generation" kann gar nicht mehr anders. Man muss als Arbeitgeber hierauf reagieren, um im Wettbewerb um den besten Nachwuchs mithalten zu können.
- Höhere Produktivität der Mitarbeiter, weil sich mit den Geräten die Möglichkeiten zur Zusammenarbeit verbessern. Das stehe im Gegensatz der früheren Befürchtung, dass die Produktivität durch zu viel privaten Gebrauch nachlasse.

Die nicht ganz so offen vorgetragenen Argumente für BYOD sind:

- Das Unternehmen kann Geld damit sparen, wenn die Mitarbeiter ihre eigenen Geräte mitbringen. Der Traum eines jeden CIOs. Und dabei geht es nicht nur um die Anschaffungskosten, sondern auch um die ganze Verwaltung, Support, etc.

- Der groß angelegte Angriff auf die Zeit zwischen Ausstempeln und Einstempeln. Wenn der Mitarbeiter sowieso mit *flat rate* immer im Internet ist, dann darf er dabei doch gerne die Firmen-E-Mails bearbeiten. Eine Trennung zwischen *business* und *private* sei eh nicht mehr so strikt wie früher, kann man da hören.

Gerade der letzte Punkt erregt bei Betriebsräten Bedenken. Nicht umsonst sind Initiativen zur Vereinbarkeit von Familie und Beruf notwendig, um bei einer übermäßigen Arbeitsbelastung ausreichend Ausgleich zu finden. Und nun droht der Einzug der Datenflut der Firmen in die Privatgeräte der Mitarbeiter, das eigene Leben zur Bannerwerbung zu reduzieren. Und die Mitarbeiter liefern hierzu sogar die eigene Infrastruktur in Form von Endgeräten und *flat rates*. Das ist nun etwas überspitzt ausgedrückt, aber ein durchaus zu beobachtender Impuls. Es wird schnell der Ruf laut, das müsse man in einer Betriebsvereinbarung regeln, ohne dass klar wäre was da denn drin stehen soll.

Ganz so eindeutig zu Lasten der vermeintlich ausgebeuteten Mitarbeiter kann das Thema allerdings nicht gesehen werden. Gerade für junge Familien ist eine solche Erreichbarkeit oft eine Erleichterung für den Alltag. Kinder wollen betreut sein – und werden auch mal krank. Man ist da oft froh, wenn die Arbeitszeiten nicht ganz so *nine to five* gelten, wie das früher mal der Fall war. Gerade wenn die klassische Aufteilung von Beruf (Mann) und Erziehung (Frau) zunehmend zum Auslaufmodell wird. Zum Problem wird das nur, wenn die Erwartungshaltung des Unternehmens nicht mit der Erwartungshaltung der Mitarbeiter zusammenpasst.

Ganz andere Themen stellen sich bei der praktischen Umsetzung einer BYOD-Initiative. Die Anbieter von Smartphones (Apple, Samsung, etc.) orientieren sich vorwiegend am Consumer-Markt. Beispielsweise entsteht beim Kauf im Apple *App-Store* immer ein Vertrag zwischen Apple und dem Nutzer. Das widerspricht eigentlich den Einkaufsregelungen in den Unternehmen, weil normalerweise nur der Einkauf solche Verträge eingehen darf. Seit kurzem bietet Apple ein „*Value Purchasing Program*", das aber im Wesentlichen den Bezahlvorgang vereinfacht. Beim Runterladen der App kommt immer noch der Vertrag zwischen Apple und dem Nutzer zustande.

Ebenso ist Regelungsbedarf hinsichtlich der eingebauten Kameras oft überfällig. In vielen Technologie-Unternehmen existiert ein Fotographie-Verbot bis hin zum Verbot, überhaupt ein Fotographie-taugliches Gerät mitzuführen. Nur sind heute quasi alle mobilen Endgeräte mit Kamera ausgestattet. In den letzten Jahren wurde das Problem bei firmeneigenen Endgeräten oft dadurch gelöst, dass die Kamera unbrauchbar gemacht wurde. Entweder über einen geschützten Administratoren-Zugang oder sogar mechanisch durch Zerkratzen der Linse. Das ist mit privaten Geräten natürlich nicht möglich. Um hier zu tragfähigen Regelungen zu kommen ist oft eine sehr breit angelegte Zusammenarbeit nötig zwischen den einzelnen Funktionen, die für Informationssicherheit im Unternehmen zuständig sind. Beispielsweise möchte kein Fahrzeughersteller zwei Monate vor der Automesse ein Bild des neuen Erlkönigs in der Zeitung haben.

Im Rahmen einer BYOD-Initiative stellen sich sogar steuerliche Fragen. Beispielsweise ist der geldwerte Vorteil durch die Nutzung des firmeneigenen WLANs zu klären. Andererseits sind die privaten Endgeräte möglicherweise steuerlich absetzbar, sofern sie auch geschäftlich genutzt werden.

Klar ist, dass in dem Thema BYOD viele Chancen aber auch manche Risiken stecken. Diese sind in einen Ausgleich zu bringen. Das kann nur geschehen, wenn eine offene Diskussion aller Beteiligten geführt wird.

Dank an Kai Nothdurft für viele hilfreiche Hinweise.

Referenzen

Tony Bradley, PCWorld: Pros and Cons of Bringing Your Own Device to Work; http://www.pcworld.com/article/246760/pros_and_cons_of_byod_bring_your_own_device_.html

automotiveDAY: Daimler adopts dual end-user device policy; March 8, 2012; http://www.automotiveit.com/automotiveday-daimler-adopts-dual-end-user-device-policy/news/id-005302

German managers worried about iPad and tablet security; September 21, 2012; http://www.automotiveit.com/german-managers-worried-about-ipad-and-tablet-security/news/id-006835

Alle wollen die Mobil-Entwickler; 27.08.2012; http://www.computerwoche.de/karriere/karriere-gehalt/2520466/index2.html

Why BYOD Won't Always Fly by Joanie Wexler; December 20, 2011; http://www.webtorials.com/discussions/2011/12/why-byod-wont-always-fly.html

IBM X-Force 2012 Mid-year Trend and Risk Report; September 2012; http://www-935.ibm.com/services/us/iss/xforce/trendreports/

Good for Enterprise; http://www.good.com/

Citrix XenApp; http://de.wikipedia.org/wiki/Citrix_XenApp

Cisco IBSG Horizons Studie; http://www.cisco.com/web/about/ac79/re/horizons.html

Christian Wege

Christian Wege, Studium und Promotion in Informatik an der Uni Tübingen. Kennt den Arbeitsalltag im Großunternehmen durch seine Tätigkeit für Daimler in Stuttgart im Bereich Unternehmensarchitektur und Innovation. Seine Schwerpunkte dort sind Open Source Governance und Mainframe-Architektur.