BYOD

Im IT-Bereich wird derzeit unter dem Schlagwort „BYOD – Bring your own device" heftig über die Vor- und Nachteile privater IT-Systeme im betrieblichen Umfeld diskutiert. Dabei ist es nichts Neues, dass Mitarbeiter ihre eigenen Werkzeuge in die Arbeit mitnehmen. Der Tenor aktueller Berichterstattungen und Diskussionsbeiträge liegt dabei in der Vermeidung respektive Schadensbegrenzung. Vorteile werden teilweise angeführt, in ihrer Wirkung aber oft reduziert. Der vorliegende Bericht zeigt anhand von Praxisbeispielen, wo die Probleme liegen, wie ihnen effektiv begegnet werden kann und welche Vorteile durch den Einsatz gemischter Infrastrukturen für Unternehmen und Mitarbeiter entstehen.

Ein neuer Hype

Die Literatur und auch renommierte Beratungs- und Analysehäuser sehen unter dem Schlagwort „Bring your own device" oder kurz BYOD einen neuen Trend auf die Unternehmen zukommen. Mitarbeiter bringen ihre persönlichen IT-Systeme – meist in Form spezialisierter mobiler Endgeräte wie Ultra-Notebooks und Tablets – in das Unternehmen und greifen damit auf unternehmensinterne Ressourcen zu.

Unweigerlich wird eine Kettenreaktion restriktiver Verhaltensmuster in Gang gesetzt. Angeführt von der typisch österreichischen Frage: „Dürfen die den das überhaupt?" kommen sicherheitsbewusste IT-Verantwortliche umgehend zum Schluss: „Nein, da könnte ja jeder kommen!". Rasch werden ein paar Regeln in Umlauf gesetzt (zu Neudeutsch: Governance rules) die derartiges Verhalten als regelwidrig verurteilen und zukünftige Ahndungen ankündigen. Für die Hierarchiekette werden ebenso rasch Bedrohungsszenarien entwickelt um die eigenen Maßnahmen zu rechtfertigen.

Diese Aktionen und Reaktionen gehen solange gut, bis jemand mit genügend Einfluss auf die IT selbst in die Lage kommt mit privaten Endgeräten auf Firmenressourcen zuzugreifen. In der Regel handelt es sich dabei um genau zwei Personenkreise: IT-Leiter und Geschäftsführer.

Ein Blick auf die Motivation der Anwender

Das Bewusstsein zum Thema wurde in letzter Zeit durch geänderte Arbeitsbedingungen (Always-On, After-Work Chilling, Networking, um nur einige zu nennen), kostengünstige mobile Multifunktionsgeräte (Smartphones, Tablets, Ultra-Notebooks, etc.) sowie vermehrter einschlägiger Anfragen in den IT-Abteilungen geschärft. Dabei ist das Phänomen nicht neu.

Private Notebooks wurden bereits in den 80ern des letzten Jahrtausends als Statussymbol in Besprechungen mitgenommen. Pager wurden durch Mobiltelefone ersetzt. Mit dem Aufkommen von USB Speichern wurden Daten vorurteilsfrei übertragen oder dienten als Plattform arbeitsunterstützender aber unternehmensfremder Programme. Zunehmendem Dokumentationsbedarf und detailverliebten Bearbeitungsprozessen setzten beherzte Anwender auch das eine oder andere Funknetzwerk unterstützend zur Seite, ohne die IT-Verantwortlichen mit Informationen zu belasten.

Folgt man der einschlägigen, meist IT-orientierten Betrachtung, bekommt man den Eindruck, das alles geschieht um dem Unternehmen zu schaden. Hinterfrägt man, wieso Anwender zu derartigen Mitteln greifen kommen rasch die Unzulänglichkeiten der IT-verantwortlichen Organisationseinheiten zu Tage:

- zu lange Reaktionszeiten
- unzumutbarer administrativer Mehraufwand
- inadäquate Betriebsausstattung

Die Motivation ist dann durchaus im Sinn des Unternehmens zu verstehen: Reduktion der Time to Market, Abbau von Overhead, Erhöhung der Produktivität durch Ressourcenoptimierung.

Weitere – unausgesprochene – Aspekte sind Prestige und Statussymbolik. Auch ist das Verständnis für die Einschränkungen durch, und bei den IT-Systemen selbst, nicht vorhanden oder ungenügend ausgeprägt.

BYOD – eine Begriffsdefinition

Es überrascht nicht weiter, dass renommierte Branchengrössen wie Gartner das Thema BYOD aufgreifen und als Trend in den Vordergrund stellen. Hersteller bieten eine schier unüberschaubare Vielfalt an Lösungen um private Endgeräte in die Unternehmens-IT einzubinden.

Tabelle 1 gibt eine Übersicht über die Hard- und Software, welche in Unternehmen eingebracht und dort genutzt werden.

Hardware	Software	Infrastruktur
• PC/Laptop/Tablet • Telefon (Smartphone) • Datenträger • USB-Stick • Zubehör	• Standard Software (zB Office) • Hilfsprogramme	• Netzwerk kompatibel (passiv, aktiv) • Server (für Arbeitsgruppen) • WLAN (Router/AccessPoint) • Webbasierende Communities (zB Xing)

Tabelle 1: Aufstellung privater Informationstechnologie

Tabelle 1 macht transparent, dass bei der Behandlung des Themas BYOD nicht ausschließlich iPhones und iPads im Fokus der Betrachtungen stehen und es damit nicht ausreicht, diese Geräte zu verbieten oder durch Installation von beschränkender Software für den Administrator beherrschbar zu machen.

> *Unter „Bring your own device" ist die Inbetriebnahme, Nutzung und Zugriff auf unternehmens-eigene Ressourcen mithilfe privater, unternehmensfremder Informationstechnologie ungeachtet der Legitimation oder Motivation durch das Unternehmen zu verstehen.*
>
> *(Eigendefinition der Autoren)*

Einen Sonderfall stellt die Integration von Unternehmenszukäufen – insbesondere kleiner Unternehmen – dar, wo der Grad individueller IT besonders hoch ist.

Spion, Spion – eine Risikobetrachtung

Nicht jeder Mitarbeiter mit einem privaten Tablet will die Firmen-IT hacken und Unternehmensdaten ausspionieren. Wie bereits oben angedeutet, sind Arbeitserleichterung und Effizienzsteigerung häufiger anzutreffende Motive. Trotzdem sind Situationen denkbar, aus welchen Unternehmen Schaden entstehen, ohne dass dabei böswillige Absicht oder auch nur Fahrlässigkeit der Betroffenen im Spiel waren. Exemplarisch stelle man sich vor, das Tablet des Geschäftsführers mit der Präsentation einer Produkteinführung wird aus dem Firmen-PKW entwendet.

Tabelle 2 beschreibt die Risiken im Zusammenhang mit beruflich genutzter privater Informationstechnologie:

Risiko	Kategorie (betrifft)
• Unautorisierte Nutzung von Netzwerkressourcen • Zugriffssicherheit	Sicherheit

• Datei (-austausch-) format (Inkompatibilitäten)
  • Datenformate
  • Visuelle Erscheinung der Dokumente (eingeschränkte Rechtsverbindlichkeit)
	Verfügbarkeit
	
	Recht

• Einbringen von Schadsoftware	Sicherheit
• Cyberwar, BOTNets	Sicherheit
• Kampf auf fremden Terrain (unbekannte HW, SW)	Sicherheit
• Urheberrechtsverletzungen	Recht
• Sonstige Rechtsverletzungen	Recht

• Lizenzverstöße
  • bewusst
  • unbewusst
	Recht

• Ressourcenmissbrauch
  • passiv
  • aktiv
	Verfügbarkeit

• Datendiebstahl (+ Spionage)	Sicherheit
• Störungen (des oder durch das Endgerät) • Erhöhte Komplexität der Unternehmens-IT Umgebung	Verfügbarkeit
• Erhöhter Know-how Bedarf • Personalkosten, Testumgebung	Know-how
• CI Aufweichung	Integrität
• Persönlicher Hardware/Software/Datenverlust	Verfügbarkeit

Tabelle 2: Risiken durch BYOD

Gemäß Tabelle 2 bedarf es keiner allzu großen Anstrengungen um beim Gedanken an private Endgeräte im Unternehmensumfeld Endzeitvisionen zu bekommen. So gesehen sind die Argumente der IT-Administratoren nicht falsch. Sie bedürfen aber einer differenzierten Risikobetrachtung um von der reinen Panikmache zu fundierten Aussagen bezüglich Risiko und Gegenmaßnahmen zu kommen.

Hurtig fortgeschritten – die Chancen von BYOD

Jedem (sinnvoll eingegangenen) Risiko steht eine Chance auf Verbesserung der Gesamtsituation gegenüber. Diese Chancen werden gerne von Herstellern und Systemverantwortlichen verkürzt dargestellt und unterbewertet. Gerade IT-Verantwortliche sollte aber die Chancen kennen und bewerten können, da sie die Aktivposten des Business Case darstellen.

Chancen	Kategorie (betrifft)
• Akzeptanz und Image	Image

• Kostenersparnis für
  • Hardware
  • Software
  • Schulungen (der Basissysteme)
	Kosten

• Innovationslanze (Innovationsvorsprung)	Kosten
• Reduziertes Innovationsrisiko	Kosten
• Rücklauf von Know-how ins Unternehmen	Kosten
• Mobile Arbeitsplätze (Flexibilisierung und Mobilisierung der Mitarbeiter)	Image
• Reduktion der unternehmensinternen Angriffsfläche	Sicherheit, Verfügbarkeit
• Kampf bewusst auf fremdes Terrain verlegen • u.a. durch bekannte, abgrenzbare Quarantänezone	Sicherheit

Tabelle 3: Chancen durch BYOD

Tabelle 3 ist zu entnehmen, dass einige Vorteile schon durch den Tatbestand privater Geräte an sich zu lukrieren sind. So sind private Endgeräte meist moderner und besser ausgestattet als nach gesamtwirtschaftlichen Gesichtspunkten ausgewählte Unternehmensgeräte. Damit einher geht eine höhere Motivation, diese Geräte zu nutzen und auch neue Lösungen auszuprobieren.

Andere Chancen sind nicht so offensichtlich umsetzbar und bedürfen einer Adaption der Unternehmens-IT. Exemplarisch seien abgekapselte Datensilos und webbasierte Unternehmensanwendungen erwähnt. Letztere substituieren kostenintensive Client-Applikationen.

Tag der offenen Tür – Sinnvolle Maßnahmen

Die Nutzung privater Informationstechnologie ist sicher gesondert zu betrachten, katastrophale Sicherheits-Tsunamis sind aber bei vernünftigem Umgang mit dem Thema BYOD nicht zu erwarten. Die Praxis zeigt allerdings immer wieder, dass der reine Einsatz von beschränkenden IT-Systemen keine Wirkung zeigt.

Als Beispiel sei ein österreichisches Großunternehmen erwähnt, wo der Vorstand Informationslecks gegenüber der Presse durch technische Hilfsmittel zu verhindern suchte. Nach dem Einsatz von Smartcard Authentisierung und Festplattenverschlüsselungen ging die Anzahl der Indiskretionen nicht zurück. Die technisch Verantwortlichen hatten nicht den Mut den wahren Sachverhalt zu kommunizieren: Die Vorstände gaben streng vertrauliche Dokumente selbst an die Presse.

In der Praxis hat sich ein Mix aus organisatorischen und technischen Maßnahmen als zielführend herausgestellt.

Organisatorisch ist eine **Bestandsaufnahme** und Inventarisierung der Ausgangspunkt. Um Auswirkungen und Risiken überhaupt einschätzen zu können bedarf es eines klaren Bildes der aktuellen IT. In der Erfahrung der Autoren ist diese Inventur vielfach unzureichend erfolgt und bedarf der Überarbeitung, Vertiefung und in Folge einer laufenden Überprüfung in Form formaler **Audits**. Insbesondere sind neben der Hardware auch Software und Lizenzen zu erfassen um später die Frage der Nutzungsrechte, Gewährleistungen und Ersatzansprüche eindeutig klären zu können

Klare **Leistungskataloge** der IT sowie vereinbarte **Service Level Agreements** helfen der IT, Sonderleistungen im Zusammenhang mit privaten Geräten transparent zu machen und gegebenenfalls intern weiterzuverrechnen. So lässt sich der tatsächliche Aufwand im Zusammenhang mit privater IT dem Nutzen gegenüberstellen, bewerten und frühzeitig Trends und Handlungsoptionen ableiten.

Zu überlegen sind auch eigene **Versicherungspakete** um im Störungs- und Problemfall unangenehme Ad-hoc Diskussionen zu vermeiden. Solche Versicherungen haben den Kostenvorteil großer Mengen und können dem Mitarbeiter als Entlohnungsergänzung angeboten werden.

Neben den hinlänglich bekannten Maßnahmen wie **Verbot** und **Vollintegration** – hier wird die private Hardware vollständig mit unternehmenseigener Software und Lizenzen ausgestattet – gibt es eine Reihe von sinnvollen technischen Maßnahmen um das Zusammenspiel zwischen privater und unternehmenseigener IT optimal zu gestalten.

Am einfachsten ist es, den Zugang über **definierte Netzwerkeinstellungen** – IP Adresse, Protokolle, Ports – zu steuern. Unter dem Gesichtspunkt „All input is evil" wird jedes Endgerät als externer Partner gesehen. Die zentrale Unternehmens-IT verhält sich wie ein abgeschlossener Datensilo.

Der Zugang über **Adaptertechnologien** kann differenzierter und vielfältiger ausfallen. Hier stehen virtuelle Maschinen, Server based Computing und Terminalserver, Hardwareverschlüsselungen, Zugangstokens sowie Portale und Inhouse Webshops bereit um eine saubere Trennung zwischen unternehmensintern servicierten und privaten, unservicierten Endgeräten zu unterscheiden.

Eine höhere Integration und damit Öffnung der Unternehmens-IT erhält man durch Einsatz von **Zertifikaten und Zugangsschlüssel**. In großen Unternehmen mit entsprechend komplexer IT-Infrastruktur sind derartige Maßnahmen alleine unzureichend. Hier sind Überwachungssysteme in Form von Intrusion Detection Systemen und konsequentem zentralem Logging notwendig um im Anlassfall rasch Ursachenforschung betreiben zu können.

Sinnvoll und oft bereits umgesetzt sind **Referenz- und Musterlösungen**. Hier wird in Form von prototypischen Szenarien eine Auswahl an Technologien akzeptiert, andere werden dagegen ausgeschlossen. So hat ein österreichischer Technologie-Marktführer die Nutzung von iPads und iPhones zuerst akzeptiert und später aktiv unterstützt. Gleichzeitig werden Android-basierte Geräte nicht unterstützt und von deren Gebrauch aktiv abgeraten. Ergänzend wurde eine auf Apple-Produkte spezialisierte Managementplattform installiert, welche die betriebliche Nutzung optimiert.

Ein Sack voller Flöhe – Erfahrungen im eigenen Haus

Die corporate quality consulting GmbH. ist ein Beratungsunternehmen mit ca. 100 langjährig erfahrenen und führungserprobten Beratern sowie einem jungen, engagierten IT-Verantwortlichen. Aufgrund der Beratungstätigkeit beim Kunden vor Ort mangelt es den Beratern nicht an guten und überzeugenden Argumenten für den Einsatz jeglicher innovativer Hilfsmittel. Für den IT-Verantwortlichen erschwert wird die Situation durch den bunt gemischten Einsatz von Hardware, Software, Peripherie und Infrastrukturkomponenten.

Um die zentralen Unternehmenskomponenten reibungslos und hochverfügbar betreiben zu können sind diese in einem zentralen, vom Rest des Unternehmens abgeschotteten Netzwerk. Der Zugang über Wireless LAN erfolgt auch in der Firmenzentrale mittels zertifikatsbasierter Authentisierung. Terrestische Netzanschlüsse

werden über VLANs kontrolliert. Jedem Mitarbeiter wird eine Firmenausstattung – bestehend aus Notebook und Mobiltelefon - bereitgestellt.

Die Nutzung externer Geräte ist prinzipiell erlaubt, das Unternehmen übernimmt hier aber keine Haftung oder Aufwände für Reparatur und Wiederherstellung. Für die Einrichtung von Datenzugängen ist der jeweilige Berater selbst zuständig.

Um die Integration auch auf firmenfremder Hardware zu ermöglichen werden virtuelle Maschinen, welche deckungsgleich zu den betriebseigenen Notebooks installiert und administriert sind, angeboten. Somit können Formatinkompatibiltäten eliminiert werden und im Problemfall steht eine Referenzinstallation zur Verfügung.

Dieser offene Umgang mit fremden und neuen Technologien erfordert von beiden Seiten Vertrauen und entsprechend Geduld. Nicht jedes Problem ist umgehend lösbar (so kann der Autor noch immer nicht mit seinem iPad über das VPN-Netz auf interne Services zugreifen). Die Offenheit, Innovationsfreundlichkeit und der damit verbundene Aufbau von Know-how führt jedoch zu einem sehr produktiven Arbeitsklima, welches die Nachteile der dezentralen Administration und sporadischer Verfügbarkeitseinschränkungen wettmacht.

Über die Autoren:

Gabriele Bolek-Fügl ist langjährige ausgewiesene Expertin im Bereich IT Sicherheit, Compliance und Governance. Sie ist Wirtschaftsprüferin und IT-Auditorin und hat bereits zahlreiche Unternehmen bei der Einführung von BYOD beraten und begleitet.

Wolf Rogner kennt die Thematik sowohl aus der Sicht des IT-Verantwortlichen als auch des Early Adopters. Im Zusammenhang mit offenen Systemen hat er bereits mehrfach praktikable und nachhaltige Lösungen entwickelt und zur Einsatzreife gebracht.