INFOWATCH®
BECAUSE YOUR DATA IS YOUR BUSINESS

www.infowatch.com

Mein Unternehmen hat BYOD – was muss ich tun?

09/2012, All about security

Arbeiten im Home Office ist seit gut zehn Jahren gängige Praxis und die geschäftliche Nutzung privater Handys eine Realität in den meisten Unternehmen. Daher ist das augenblicklich viel zitierte Bring your own Device (BYOD) eigentlich kein neues Thema mehr.

In den Medien ist der Begriff BYOD allerdings bis vor einem Jahr faktisch unbekannt gewesen und nun explodiert eine Flut von immer neuen Studien dazu, **was hat sich also geändert?**

Wenn das Thema an sich nicht neu ist, dann müssen es die Gefahren sein, die durch BYOD entstehen. Und in der Tat hat sich die Bedrohungslage durch BYOD vor allem in den letzten Jahren deutlich verschärft. So sind heute fast alle Daten digitalisiert, private Breitband-Verbindungen sind mittlerweile Standard und die meisten Angestellten besitzen leistungsfähige Smartphones. Diese IT-Aufrüstung im Privaten führte dazu, dass nicht wie bislang private Dinge am Arbeitsplatz erledigt wurden, weil dort die leistungsfähigere Hardware verfügbar war, sondern dass jetzt die Arbeit auf die oft besseren privaten Geräte ausgelagert wird. Während Unternehmen lange Zeit die Vorteile von BYOD nutzen konnten ohne darin ein großes Risiko zu sehen, sind USB-Sticks auf die mittlerweile ganze Firmen-Datenbanken passen, Notebooks, die Viren in Firmen einschleppen können und Smartphones, die samt und sonders mit hochauflösenden Kameras ausgestattet sind, ein zunehmendes Risiko für viele Unternehmen.

BYOD deshalb schlichtweg zu verbieten, ist jedoch für die meisten Unternehmen keine Option, da es weder realisierbar ist, alle Smartphones, Tablets und USB-Sticks aus dem Unternehmen zu verbannen, noch aus betrieblicher Sicht wünschenswert. Lösungen müssen folglich gefunden werden, und bevor diese aus Patentrezepten bestehen, sollte sich der IT-Verantwortliche jedoch einen Augenblick Zeit nehmen, um sich zunächst mehrere Facetten von BYOD vor Augen zu führen.

Die Risiken und Nebenwirkungen

Grundsätzlich ist das bestehende Risiko beim Einsatz privater IT- und Telekommunikations-Geräte längst bekannt und häufig liest man in den Medien die Wiederholung recht ähnlicher Szenarien. Mit am stärksten von den Medien propagiert, sind Fälle von Missbrauch und Spionage, etwa wenn ein Mitarbeiter dank seines Breitband-Anschlusses und entsprechender Zugangsdaten für sein Home Office problemlos ganze Images entwenden kann. Gerade Personaldaten haben einen gut etablierten Schwarzmarkt und der verantwortliche Mitarbeiter hat oft gute Chancen unerkannt zu bleiben.

Allerdings gibt es jenseits der medialen Aufmerksamkeit andere Ursachen, die weit größere Bedrohungen für die Datensicherheit darstellen: Bequemlichkeit und Sorglosigkeit im Umgang mit Daten sind dafür verantwortlich, dass sich nach Statistiken des aktuellen DLP-Jahresreports von InfoWatch täglich rund 200 Vorfälle von Data Leakage ereignen. So werden beispielsweise betriebliche E-Mails nicht nur mit dem Handy abgerufen, sondern auch auf selbigem gespeichert, oft nur, weil das Smartphone werksseitig so eingestellt war. Genauso werden Daten oftmals zur Bearbeitung über ungesicherte USB-Sticks oder über

nicht verschlüsselte Tablets oder Notebooks mit nach Hause genommen. Ein Verlust der Hardware bedeutet dann meist, dass diese Daten in fremde Hände geraten. Darüber hinaus kann selbst ein sorgfältiger Umgang mit Daten nicht verhindern, dass private Hardware gegebenenfalls anfälliger für Trojaner und Spyware ist, und somit die Verwendung von privaten Devices ein höheres Risiko birgt als die IT-Abteilung ahnt.

Solche Situationen verlangen folglich, betriebliche Richtlinien, die die Risiken kalkulierbar und den Einsatz privater Hardware planbar machen. Mag bis zu diesem Punkt noch Einigkeit über BYOD herrschen, so divergieren die Meinungen spätestens dann, wenn es um die konkreten Maßnahmen zur Bekämpfung geht.

Die Packungsbeilage

Die wenigsten Unternehmen können sich auf jahrelange Erfahrung im Umgang mit BYOD berufen. Viel eher versucht man mit Patentrezepten der Situation Herr zu werden. Klassiker der Lösungsversuche ist nach wie vor die Policy, die den Mitarbeiter zu mehr Sorgfalt ermahnt. Je nach Unternehmensphilosophie wird der Mitarbeiter dabei zur Unterschrift genötigt, mit der er für eventuelle Schäden haftet, oder aber es wird lediglich moralisch an ihn appelliert. Beides ist eher eine betriebliche Verzweiflungsmaßnahme, die keinen wirksamen Schutz gegen die von BYOD ausgehenden Gefahren bietet.

Ein weiteres Patentrezept ist das schlichte Verbot von BYOD, auch dann, wenn dies weder realisierbar, noch kontrollierbar und für die Mitarbeiter auch oft nicht nachvollziehbar ist. Häufig fehlt bei einem solchen Verbot bereits die Definition, was unter BYOD konkret zu verstehen ist.

Dass solche Patentrezepte nach wie vor das Mittel der Wahl zu sein scheinen, hat zwei Ursachen: Zum einen lässt sich die Wirksamkeit solcher "Lösungen nach Vorschrift", und sei sie noch so gering, nicht ganz von der Hand weisen und derjenige, der sich für eine solche Lösung verantwortlich zeigt, kann folglich immer auch auf einen minimalen Erfolg seiner Lösung verweisen. Zum anderen offenbaren solche Lösungen viel eher die Hilflosigkeit des Unternehmens, die Situation adäquat zu erfassen und angemessen zu reagieren. Woran soll sich folglich ein Unternehmen orientieren, das eine angemessene Lösung für das Problemfeld BYOD sucht?

Der Arzt oder Apotheker empfiehlt

Während gegen Hacker und Phishing inzwischen selbstverständlich externe IT-Security-Spezialisten zu Rate gezogen werden, scheint BYOD nach wie vor etwas zu sein, bei dem sich Unternehmen fest vorgenommen haben, es auf eigene Faust zu lösen. Spezialisten, die individuelle auf das Unternehmen abgestimmte Lösungen bieten, kommen derzeit vor allem aus dem DLP-Bereich, was nicht weiter wundert, denn hier war BYOD längst ein Thema noch bevor es den Begriff gab. Eines dieser Unternehmen ist der **deutsche Security-Anbieter EgoSecure** , der als Hilfestellung für Unternehmen einen Leitfaden für BYOD-Konzepte bereithält. Dieser Leitfaden wurde vom Unternehmen als die CAFE-Philosophie bezeichnet. Dahinter stecken die vier Schwerpunkte **Access Control, Audit, Filter und Encryption**, die das Unternehmen als unverzichtbar für jede geeignete BYOD-Richtlinie ansieht.

Mit **Access Control** wird dabei die Kontrolle der Datenwege bezeichnet. IT-Administratoren müssen jederzeit bestimmen können, welcher Account welche Daten über welche Kanäle transportieren darf. Ein mitgebrachter USB-Stick ist ungefährlich, wenn bestimmte Daten prinzipiell nicht auf externe Datenträger gespeichert werden können. Control so verstanden, bietet hier auch Schutz der weit über BYOD hinausreicht. Notwendig um eine solche Kontrolle der Datenwege effektiv zu implementieren ist es jedoch, Daten zu klassifizieren und in die gesamte IT-Infrastruktur eine Software zu implementieren, die die Datenwege kontrolliert. Eine Richtlinie, die BYOD schlicht verbietet und hofft damit die Datenwege kontrollieren zu können, ist nur ein schwacher Ersatz.

Eng in Zusammenhang mit Control steht **Audit**. Wenn trotz Control offensichtlich gegen die Sicherheitsbestimmungen des Unternehmens mutwillig verstoßen wurde, dann stellt sich – vor allem wenn Schaden entstand – die Frage nach den Verantwortlichen. Dieser Frage auf den Grund zu gehen setzt

voraus, dass erfasst wurde, wer wann mit welchen Daten was gemacht hat. Damit hieraus keine Mitarbeiter-überwachung wird, muss eine gute Software Sicherheitsmechanismen wie beispielsweise das Vier-Augen-Prinzip haben, um zu gewährleisten, dass nur in begründeten Fällen Einblick in diese Daten gewährleistet wird. Üblicherweise verfügen daher Betriebsrat und beispielsweise der Personalverantwortliche über unterschiedliche Passwörter, die in solchen Fällen gemeinsam eingegeben werden müssen, um Einblick in den Schaden zu bekommen.

Eine Software, die Datenwege überwachen und Verstöße feststellen kann, setzt voraus, dass Daten klassifiziert wurden. Wenn aber Daten klassifiziert wurden, ist das **Filtern von Daten** nur noch ein kleiner Schritt. Filtern geht in diesem Zusammenhang jedoch über Kontrolle der Datenwege hinaus. Während Kontrolle vor allem bedeutet, dass Firmeninterna nicht auf private Devices auswandern, kann effektives Filtern umgekehrt auch gewährleisten, dass keinerlei betriebsfremde Daten unautorisiert einwandern. Dieser Punkt betrifft die gern unterschätzte Gefahr, dass eben nicht die Nutzer privater Devices die Gefahrenquelle darstellen, sondern die Devices selber. Mit Trojanern und Spyware infizierte Devices gefährden nicht nur die Daten auf den Geräten selbst, sondern auch das Netzwerk, an das sie angeschlossen werden.

Waren die bislang vorgebrachten drei Aspekte von BYOD-Richtlinien eher zur Regelung angedacht, welche Daten überhaupt abwandern oder abgespeichert werden dürfen, und welche Daten prinzipiell nicht mit BYOD in Berührung kommen dürfen, so setzt der vierte Aspekt direkt an den Daten an, die zulässigerweise und gewollt auf private Devices überspielt werden: **Encryption**. Der DLP-Jahresreport von InfoWatch zeigt, dass jedes Jahr ca. ein Viertel aller Daten verloren gehen, weil Datenträger oder Hardware gestohlen oder verloren wurden, auf denen sich unverschlüsselte Informationen befanden. Dieser Verlust von Daten lässt sich leicht verhindern, indem eine grundsätzliche Verschlüsselungspflicht für Daten implementiert wird. Diese kann dann natürlich auch automatisiert werden. Verlorene Datenträger würden dann nur noch einen materiellen Schaden für das Unternehmen bedeuten.

Was grundsätzlich den Einsatz von Experten bei der Umsetzung von BYOD-Richtlinien ratsam macht, ist jedoch ein Kriterium, an dem sich jede Lösung von BYOD messen lassen muss: **Wenn der Umgang mit BYOD wirksam geregelt werden soll, muss die Lösung von der Belegschaft akzeptiert werden.** Nicht akzeptierte Lösungen werden umgangen. Dies kann natürlich durch entsprechenden technischen und personellen Aufwand verhindert werden, allerdings leidet die Mitarbeiter-Akzeptanz zunehmend, was sich spätestens in der Produktivität niederschlägt.

Mit BYOD muss sich ungeachtet der Branche und der Größe jedes Unternehmen auseinandersetzen. BYOD ist ein komplexes Problem, welches weder vermieden noch ausgeblendet werden kann. Patentrezepte, egal ob aus blindem Aktionismus oder aus mangelndem Verständnis für die Situation, werden der Situation oft nicht gerecht. Viele Unternehmen sind daher gut beraten, wenn sie bei der Suche nach einer geeigneten Strategie auf fremden Sachverstand zurückgreifen. Die vier genannten Eckpfeiler einer BYOD-Lösung sollten den Verantwortlichen verdeutlichen, welche Aspekte eine nachhaltige BYOD-Lösung berücksichtigen muss.

http://www.all-about-security.de/security-artikel/endpoint-sicherheit/mobile-computing-und-pdas/artikel/14595-mein-unternehmen-hat-byod-was-muss-ich-tun/