SOPHOS
Security made simple.

Chancen und Risiken von BYOD

Strategien zur Sicherung der Smartphones, Laptops und Tablet-PCs Ihrer Mitarbeiter

Von **Gerhard Eschelbeck**, Chief Technology Officer

Bring Your Own Device (BYOD) ist in der Arbeitswelt von heute schon eher die Regel als die Ausnahme. BYOD ist praktisch für Ihre Endbenutzer. Aber welche Auswirkungen hat dieses Arbeitsmodell auf die Sicherheit in Ihrem Unternehmen? In diesem White Paper erfahren Sie, welche Chancen und Risiken BYOD birgt und wie Sie in Ihrem Unternehmen BYOD einführen können, ohne die Sicherheit Ihrer Daten zu gefährden.

Die Bedeutung von BYOD für Ihr Unternehmen

Heutzutage stehen führende IT-Unternehmen beim Thema Sicherheit vor vielfältigen Herausforderungen und müssen schnell auf Veränderungen reagieren. Immer mehr neue Sicherheitsprobleme müssen mit zunehmend knappen Ressourcen gelöst werden. Um wettbewerbsfähig zu bleiben, müssen Unternehmen ihren Mitarbeitern die neuesten und fortschrittlichsten Technologien zur Verfügung stellen. Sie müssen Unternehmens-, Kunden- und Mitarbeiterdaten schützen und gleichzeitig Angriffe von Cyberkriminellen abwehren.

Dank neuer Technologien gibt es heute neue Arten des Datenzugriffs, neue Gerätetypen sowie Alternativen zur herkömmlichen PC-Plattform. Tim Cook, der CEO von Apple, nennt diese Entwicklung „Post-PC-Ära".[1]

Dieser Trend hin zu BYOD ist an modernen Arbeitsplätzen immer mehr die Regel statt die Ausnahme.

BYOD gilt nicht nur für PCs. Mitarbeiter verwenden für ihre Tätigkeit u. a. auch Smartphones, Tablet-PCs, BlackBerrys und Ultraleicht-Notebooks. Das BYOD-Konzept wird auch immer mehr auf Software und Services ausgeweitet, da Mitarbeiter internetbasierte Cloud-Dienste und andere Tools verwenden.

Die technischen Unzulänglichkeiten, die BYOD noch vor ein paar Jahren unrealistisch erscheinen ließen, sind heute behoben und die Tools erfreuen sich großer Beliebtheit.

Zu diesen Tools zählen:

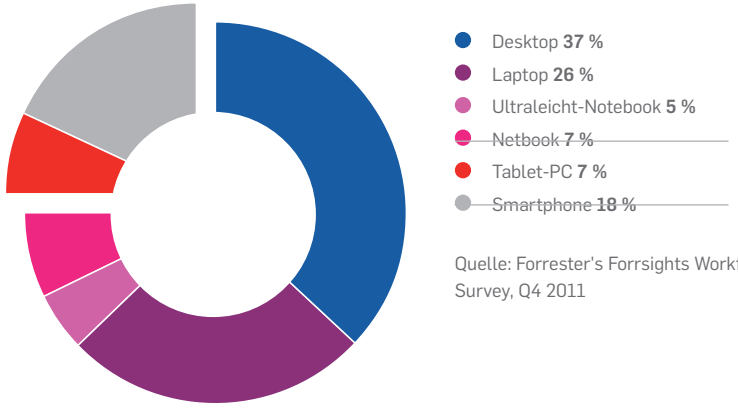
1. Internet: Das Internet bietet heute einzigartige Zugriffsmöglichkeiten auf jegliche Geschäfts-, Finanz-, Kundensupport-, Vertriebs- oder Technologie-Anwendungen.

2. WLAN: Egal, wo Sie sind oder welches Gerät Sie verwenden, breit angelegte WLAN-Netze bieten Ihnen Zugriff auf Ihre Unternehmensinfrastruktur.

3. Mobile Geräte: Moderne Geräte sind funktionsreicher, preisgünstiger und kleiner geworden, bieten große Speicher und lange Akkulaufzeiten.

1. „The post-PC world is real and it's here", *The Globe and Mail,* http://www.theglobeandmail.com/technology/gadgets-and-gear/the-post-pc-world-is-real-and-its-here/article4098023/

Eines von vier Geräten am Arbeitsplatz ist entweder ein Smartphone oder ein Tablet-PC.



Quelle: Forrester's Forrsights Workforce Employee Survey, Q4 2011

Die Bedeutung von BYOD für die Sicherheit

Die Annahme, man könne Sicherheitsprobleme lösen, indem man die Nutzung privater Geräte einfach verbietet, ist sehr riskant. Denn Ihre Mitarbeiter werden letztlich doch ihre privaten Geräte verwenden – ohne jegliche Kontrolle durch das Unternehmen und ungeachtet Ihrer Sicherheitsrichtlinien.

Egal, was Sie von BYOD halten, und wie auch immer Sie es implementieren – IT-Manager sollten dabei vorgehen wie bei der Einführung jeder neuen Technologie: mit einer kontrollierten, planbaren Bereitstellung.

Stellen Sie sich folgende Fragen:

1. Wer ist Eigentümer des Geräts? Dies hat sich im Laufe der Zeit geändert. Früher gehörten die Geräte dem Unternehmen. Beim BYOD-Konzept sind die Benutzer Eigentümer der Geräte.

2. Wer verwaltet das Gerät? Diese Frage war früher einfach zu beantworten. Heute kann es der Benutzer oder das Unternehmen sein.

3. Wer sichert das Gerät? Diese Verantwortung übernimmt der Benutzer nicht automatisch, nur weil das Gerät ihm gehört. Schließlich sind die auf dem Gerät gespeicherten Daten Unternehmenseigentum.

Die Antworten auf diese Fragen sind grundlegend für die Einschätzung von Risiken und Vorteilen, die BYOD mit sich bringt.

Es steht allen Unternehmen frei, je nach Unternehmenskultur und rechtlichen Anforderungen das BYOD-Konzept in dem Rahmen zu implementieren, in dem es ihnen vernünftig erscheint. Manche Unternehmen schätzen das Risiko als zu groß ein, so dass sie sich gegen ein BYOD-Programm entschieden haben.

Im Mai 2012 hat IBM aufgrund von Datensicherheitsbedenken seinen 400.000 Mitarbeitern die Verwendung von zwei beliebten Verbraucheranwendungen untersagt: Das Unternehmen verbot sowohl den Cloud-Storage-Dienst Dropbox als auch Siri, den persönlichen Assistenten von Apple für das iPhone. Siri erkennt gesprochene Anfragen und sendet diese an die Apple-Server, wo sie in Text umgesetzt werden. Außerdem kann Siri per Spracheingabe SMS-Nachrichten und E-Mails erstellen. Diese Nachrichten könnten jedoch vertrauliche, rechtlich geschützte Daten enthalten.[2]

Letztendlich hängt der Erfolg Ihres BYOD-Programms davon ab, ob Ihre Mitarbeiter bereit sind, ihre Privatgeräte im Rahmen der Unternehmensvorschriften zu verwenden. Die Sicherheitsverfahren und -richtlinien Ihres Unternehmens sollten festlegen, ob und wie BYOD implementiert wird.

Sie müssen in der Lage sein, Sicherheitsbestimmungen auf Geräte-Ebene durchzusetzen und Ihr geistiges Eigentum zu schützen, wenn Geräte verloren gehen oder gestohlen werden.

BYOS: Bring Your Own Software

Dieselben Technologien, durch die es zur BYOD-Wende kam, bieten den Benutzern auch Zugriff auf unternehmensfremde Software. Dafür steht die Bezeichnung „Bring Your Own Software“ (BYOS).

Endbenutzer können dank kostenloser Cloud-Storage-Anwendungen gemeinsam an großen Dokumenten arbeiten oder diese weiterleiten. Diese Dokumente können jedoch Daten enthalten, für die strenge Datenschutzrichtlinien gelten, die in der Cloud nicht in jedem Fall umgesetzt werden können – mit der Folge, dass Ihre Daten möglicherweise nicht ausreichend geschützt werden.

Sie sollten daher prüfen, wie Cloud-Storage-Anbieter Ihre Unternehmensdateien übermitteln und speichern. Stellen Sie folgende Fragen:

- Wie werden die Daten verschlüsselt?
- Wird für alle Kunden dieselbe Verschlüsselung verwendet?
- Wer hat Zugriff auf den Schlüssel zur Dechiffrierung der Daten?
- Werden die Daten bei Strafandrohung an Behörden herausgegeben?
- In welchen Ländern stehen die Server, auf denen die Daten gespeichert werden?
- Sichern Sie Ihren Kunden zu, dass deren Daten in bestimmten Ländern nicht gespeichert werden?

Laden Sie auf sophos.de das White Paper „Probleme mit Dropbox?“ herunter.

2. „IBM: Sorry, Siri. You're Not Welcome Here,“ InformationWeek, http://www.informationweek.com/news/security/mobile/240000882

So sichern Sie BYOD-Geräte

Um BYOD-Geräte zuverlässig zu sichern, benötigen Sie ebenso klare Sicherheitsmaßnahmen wie für alle anderen Geräte, die sich bereits in Ihrem Netzwerk befinden. Folgendes zählt zu diesen Sicherheitsmaßnahmen:

- Durchsetzung strenger Passwörter auf allen Geräten
- Virenschutz und Data Loss Prevention (DLP)
- Vollständige Verschlüsselung von Festplatten, Wechseldatenträgern und Cloud Storage
- Mobile Device Management (MDM) zum Löschen vertraulicher Daten, falls ein Gerät verloren gegangen ist oder gestohlen wurde
- Application Control

Eine Verschlüsselung sollte grundsätzlich sowohl bei der Übertragung als auch bei der Speicherung von Daten stattfinden. Mit sicheren Passwörtern auf Ihren Geräten wird es für Unbefugte sehr schwierig, sich Zugriff auf Ihre Daten zu verschaffen. Falls doch ein Gerätepasswort geknackt wird, haben Sie durch die Verschlüsselung der Daten auf dem Gerät eine zweite Sicherheitsbarriere, die ein Hacker erst einmal durchdringen muss, um Ihre Daten zu stehlen.

Erklären Sie Ihren Mitarbeitern, dass zusätzliche Sicherheitsmaßnahmen sinnvoll sind, da sie die Nutzung privater Geräte am Arbeitsplatz ermöglichen. Indem ein Benutzer sein Gerät mit einem Passwort schützt, zeigt er, dass er Verantwortung für den Schutz seiner Daten übernimmt.

Zusätzlich zum Schutz durch Passwörter und Antivirus-Software sollten Sie für BYOD-Geräte eine benutzerdefinierte Application Control einführen. Wenn den Mitarbeitern im internen Netzwerk Anwendungen zur Verfügung stehen, sollten sie remote über eine VPN-Verbindung oder per E-Mail-Software auf diese zuzugreifen können.

Ein erfolgreiches BYOD-Programm ermöglicht Ihren Benutzern einerseits, auch außerhalb der Arbeitszeiten produktiv zu sein, und andererseits auch die Dinge zu tun, die ihnen Freude bereiten, wenn sie gerade nicht arbeiten, z. B. ihren Status aktualisieren oder ein interaktives Spiel spielen.

Egal, welche Entscheidung Sie in Bezug auf Ihre BYOD-Richtlinien treffen: Stellen Sie sicher, dass diese durchsetzbar sind und dass sie der IT ermöglichen, Software remote bereitzustellen.

Festlegen von Richtlinien und Compliance-Standards

Bei der Formulierung Ihrer Richtlinien müssen Sie darauf achten, dass diese die besonderen Anforderungen im Bereich BYOD adressieren. Sollen Ihre Richtlinien beispielsweise die Nutzung aller aktuell erhältlichen Geräte ermöglichen? Oder möchten Sie nur Geräte zulassen, die bestimmte Hardware und Software verwenden? Wie sieht es mit Geräten aus, die noch nicht erhältlich sind, aber vielleicht in den nächsten Jahren auf den Markt kommen?

Der Markt für mobile Handheld-Geräte entwickelt sich schnell, und ständig kommen neue Versionen und neue Hersteller dazu. Deshalb sollten Ihre BYOD-Richtlinien so formuliert sein, dass sie bei Veränderungen leicht angepasst werden können. Halten Sie strategische Richtlinien schriftlich fest und orientieren Sie sich dabei daran, wie der heutige Stand der Technik ist und was Sie in Zukunft an neuen Geräten erwarten. Führen Sie außerdem ein System ein, das Ihre Richtlinien durchsetzt und so für eine

einfache Verwaltung, Kontrolle und Sicherheit sorgt, die bei Bedarf auch einer externen Prüfung standhält.

Eine Lösung, mit der es möglich ist, die Geräte remote zu verwalten, kann eine große Hilfe bei der Pflege der Sicherheitsrichtlinien sein. Denn diese müssen permanent überprüft und auf dem aktuellem Stand gehalten werden, insbesondere wenn Sie in einer Branche mit strengen Compliance- und Prüfungsstandards tätig sind.

Ebenfalls sehr hilfreich ist es, wenn Sie einen genauen Überblick über die Verträge haben, unter denen die mobilen Geräte der Mitarbeiter laufen. So können Sie eventuell Verträge mit günstigeren Konditionen finden und dadurch die Kosten senken. Für die Endbenutzer kann es vorteilhaft sein, die Hotspot- oder Tethering-Optionen von Datentarifen in Anspruch zu nehmen. Nutzen Sie für private Wi-Fi-Geräte statt Internet-Pauschaltarifen für Home Offices lieber reine Datentarife.

Die 7 Schritte zu einem BYOD-Sicherheitsplan

Die Sicherheit Ihres Unternehmens muss unter einem BYOD-Programm nicht im Geringsten leiden. Es kommt nur auf die richtige Planung an. Die könnte z. B. wie folgt aussehen:

1. Finden Sie heraus, welche Risiken durch BYOD entstehen

- Ermitteln Sie, wie diese Risiken Ihr Unternehmen beeinträchtigen könnten
- Ordnen Sie die Risiken den entsprechenden Richtlinien zu (sofern dies sinnvoll ist)

2. Stellen Sie für die Implementierung von BYOD ein Experten-Gremium aus folgenden Mitgliedern zusammen

- Interessenvertreter des Unternehmens
- Interessenvertreter der IT
- Interessenvertreter des Datenschutzes

3. Entscheiden Sie, wie die Richtlinien für Geräte, die auf Ihr Netzwerk zugreifen, durchgesetzt werden sollen

- Für Mobilgeräte (Smartphones)
- Für Tablet-PCs (z. B. iPad)
- Für Mobilcomputer (Laptops, Netbooks, Ultrabooks)

4. Erstellen Sie einen Projektplan mit folgenden Funktionen

- Remote-Geräteverwaltung
- Application Control
- Richtlinienübereinstimmung und Prüfungsberichte
- Daten- und Geräteverschlüsselung
- Erhöhung der Sicherheit von Cloud Storage
- Entfernen aller Daten von Geräten, die außer Betrieb genommen werden
- Entzug des Zugriffs auf Geräte, wenn der Endbenutzer nicht mehr Mitarbeiter ist, sondern Gast
- Entzug des Zugriffs auf Geräte, wenn dem Mitarbeiter gekündigt wurde

5. Vergleichen Sie die Lösungen

- Vergleichen Sie, wie stark die Auswirkungen der jeweiligen Lösungen auf Ihr jetziges Netzwerk sind
- Fragen Sie sich, wie Sie bereits vorhandene Technologien verbessern können, bevor Sie über weitere Schritte nachdenken.

6. Implementieren Sie die Lösungen

- Beginnen Sie mit Pilotgruppen in den Abteilungen der verschiedenen Interessenvertreter
- Fügen Sie gemäß Ihrer organisatorischen Anforderungen Pilotgruppen in anderen Abteilungen hinzu
- Machen Sie das BYOD-Programm schließlich für alle Mitarbeiter zugänglich

7. Bewerten Sie die Lösungen in regelmäßigen Abständen neu

- Ziehen Sie Anbieter und Berater Ihres Vertrauens hinzu
- Nutzen Sie Roadmaps, wenn der nächste Evaluierungszeitraum beginnt
- Ziehen Sie ggf. kostensparende Gruppentarife in Betracht

Bei korrekter Implementierung kann ein BYOD-Programm Kosten reduzieren und gleichzeitig Produktivität und Gewinn erhöhen. Da BYOD in den IT-Abteilungen immer mehr die Regel wird, sollte das Thema Sicherheit an erster Stelle stehen, sowohl bei den Benutzern als auch bei den IT-Administratoren.

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0 | +49 721 255 16 0
E-Mail: sales@sophos.de

7.13.GH.wpna.simple

SOPHOS