BYOD

Fabian Gröger

28.03.2018

Contents

1 Verantwortlichkeiten **2**
1.1 Geschäftsleitung . . . 2
1.2 IT . . . 2
1.3 Mitarbeiter . . . 2

2 Sicherheitsrisiken **3**
2.1 Verloren oder gestohlen . . . 3
2.2 Drahtlose Verbindungen . . . 3
2.3 Kein Passwortschutz . . . 3
2.4 Datenschutzverletzung über Mobile Apps . . . 4
2.5 Nicht verschlüsselte Daten und Verbindungen . . . 4

3 Sicherheitsmassnahmen **4**
3.1 Mobile Geräte sichern . . . 4
3.2 Geräteverwaltung . . . 4
3.3 Geräte verschlüsseln . . . 5
3.4 Mobile Antivirenprogramme . . . 5
3.5 Datensicherheit über die Cloud . . . 5
3.6 Trennung private und berufliche Daten und Anwendungen . . . 5
3.7 Kontinuierliche Risikobewertung . . . 6

4 Vereinbarungen **6**
4.1 Datensicherheit . . . 6
4.2 Mitteilungspflicht . . . 6
4.3 Haftung . . . 7
4.4 Steuerrechtliche Fragen . . . 7
4.5 Arbeitsrechtliche Fragen . . . 7

5 Vorgehen beim Erstellen einer Police **7**

6 Alternativen **8**
6.1 Corporate Owned Personally Enabled (COPE) . . . 8
6.2 Choose Your Own Device (CYOD) . . . 8

6.3 Bring Your Own Connection (BYOC) 9
6.4 Bring Your Own Software (BYOS) 9

7 Schlusswort **9**

8 Quellenverzeichnis **9**

9 Anhang **9**

9.1 Beispiel Police **9**

---

1 Verantwortlichkeiten

Bei den Verantwortlichkeiten für das Erstellen und Umsetzen eines sicheren BYOD-Konzept sollte klar unterschieden werden, was in der Verantwortung der Mitarbeiter, der Geschäftsleitung und der IT liegt.

1.1 Geschäftsleitung

Die Geschäftsleitung sollte von Anfang an, die treibende Macht sein und alles ins Rollen bringen. Wichtig ist auch, dass sie sich genug Zeit nehmen um eine überstürzte Einführung zu verhindern. Sie ist dafür zuständig, dass in ihrem Betrieb BYOD sicher und überwacht stattfindet, um somit die bestmöglichen Resultate für die Mitarbeiter und das Unternehmen zu erzielen. Der Vorstand sollte Expertengruppen einberufen und mit ihnen ein Konzept entwickeln, was für den Betrieb am besten passt und die meisten zielgerichteten Resultate erzielt.

1.2 IT

Die IT ist zuständig für die Bereitstellung und Wartung der Software, die im Konzept definiert wurde. Ausserdem sollte die IT eine kontinuierliche Risikobewertung machen und die Geschäftsleitung über den Stand informieren. Ein weiterer wichtiger Punkt, ist das Schulen der Mitarbeiter im Umgang mit der Software und ihren eigenen Geräten. Die IT ist auch für die Überwachung des Systems zuständig, sie muss immer wissen was gerade im System passiert und wenn neue mögliche Sicherheitsrisiken aufkommen.

1.3 Mitarbeiter

Die Mitarbeiter sollten durch die Schulung der IT eine gewisse Sorgfalt gelernt haben mit dem Umgang der geschäftskritischen Daten und ihren mobilen Geräten,

und diese auch gekonnt im Unternehmen und privat anwenden. Ausserdem liegt in jedem Mitarbeiter die Verantwortung die IT darüber zu informieren, wenn ein Gerät defekt, verloren oder gestohlen wird.

2 Sicherheitsrisiken

Chance oder Risiko? BYOD ist beides. Chancen sind die Abläufe zu verändern und zu vereinfachen, Mitarbeiter Zufriedenheit zu erhöhen und Anschaffungskosten für mobile Endgeräte zu minimieren. Ein Risiko besteht, wenn das eigentliche Potenzial von "Bring your own device" durch eine überstürzte und unbedachte Einführung unterwandert wird. Problematisch wird es, wenn Auswirkungen auf die bestehende Netzwerk-Infrastruktur nicht berücksichtigt werden und somit grosse Sicherheitsrisiken entstehen.

2.1 Verloren oder gestohlen

Der Hauptunterschied zur fest am Arbeitsplatz installierten Hardware ist, dass Mobilgeräte schneller verloren oder gestohlen werden können. Und wenn personenbezogene Daten mit vertraulichen Firmendaten in einem Gerät vermischt werden, ist das Risiko, dass diese Informationen im Falle eines Diebstahls an die Öffentlichkeit gelangen, inzwischen eine beängstigende Möglichkeit. Das passiert einem Desktop-PC eher selten. Zudem können die Daten leichter Schaden nehmen, ausgespäht oder anderweitig missbraucht werden, was auch für die weitverbreitete Nutzung von USB-Sticks und anderen portablen Speichermedien gilt, welche unterbunden werden sollte.

2.2 Drahtlose Verbindungen

Einen zusätzlichen Angriffspunkt bieten die drahtlosen Netzverbindungen, die Angreifern prinzipiell einen leichteren Zugang ermöglichen als ein Kabel, das gewöhnlich physikalisch geschützt verläuft. Hier besteht die Gefahr des Datenmissbrauchs, der Fälschung oder Löschung von Daten sowie der Manipulation von Systemen.

2.3 Kein Passwortschutz

Viele Benutzer schützen ihre persönlichen Geräte oder die Anwendungen auf ihren Geräten nicht wirklich mit sicheren und ändernden Passwörtern. Oder, wenn sie es tun, neigen sie dazu, aus Bequemlichkeit einfache Passwörter zu wählen. Diese Geräte sind bei Diebstahl oder Hacking leicht zu kompromittieren und liefern ein grosses Risiko, (welches leicht behoben werden kann.)

2.4 Datenschutzverletzung über Mobile Apps

Es gibt unzählige schädliche Apps, deren Ziel es ist, nicht nur die Gerätesoftware zu beschädigen, sondern auch private Daten auf dem Gerät zu hacken und darauf zuzugreifen. Und da ihre personenbezogenen und Firmendaten auf gleiche Weise behandelt werden, laufen beide Gefahr kompromittiert zu werden. Selbst wenn eine App vom Unternehmen bereitgestellt wird, ist sie, wenn keine Sicherheitsvorkehrungen in der App enthalten sind, immer noch anfällig für Angriffe.

2.5 Nicht verschlüsselte Daten und Verbindungen

Ihre Daten, einschließlich Sprachnachrichten, gehen ohne Schutz oder Sicherheitsvorkehrungen durch das öffentliche Internet. Sie können während der Übertragung oder im gespeicherten Zustand abgefangen werden.

3 Sicherheitsmassnahmen

Um möglichst alle dieser Sicherheitsrisiken abzudecken, werden in diesem Abschnitt die Sicherheitsmassnahmen zu den oben genannten Risiken aufgezeigt und erklärt. Die Sicherheitsmassnahmen sollte man kontinuierlich überprüfen. Dabei sollte kontrolliert werden ob man alle Risiken abdeckt und keine neuen Risiken entstanden sind, denn es ist ein ständiger Prozess alle Sicherheitsrisiken zu kennen und zu schliessen.

3.1 Mobile Geräte sichern

Die meisten Sicherheitsrisiken können durch die Sicherung des mobilen Geräts selbst behoben werden. Das Unternehmen sollte in eine MDM-Lösung (Mobile Device Management) investieren, die Sicherheitsrichtlinien, Benutzerverwaltung und Ressourcenverwaltung durchsetzen und sicherstellen kann, dass nur zugelassene Geräte auf ihr Netzwerk und ihre Ressourcen zugreifen können. Wichtig ist auch eine starke Verschlüsselung, um die Netzwerkinfrastruktur und die Daten beim Durchgang durch das öffentliche Internet zu schützen.

3.2 Geräteverwaltung

Mit einer mobilen Geräteverwaltung können die mobilen Geräte mit einem Passwort geschützt, lokalisiert und auf die Werkseinstellung zurückgesetzt werden, damit keine Daten an Dritte weitergegeben werden, vor allem beim Verlust der Geräte. Gleichzeitig kann der Administrator persönliche Kontakte, Mails

und Notizen wiederherstellen und über ein zentrales System verwalten. Durch passwortgeschützte Bildschirmsperren wird das Geräte zusätzlich gesichert.

3.3 Geräte verschlüsseln

Der Verlust oder Diebstahl eines Note- oder Ultrabooks, eines Smartphones, Tablets oder auch nur eines USB-Sticks führt zu einem materiellen Schaden. Aber dieser Verlust steht in keinem Verhältnis zu dem Schaden, der einer Firma dadurch entstehen kann, wenn sich auf dem jeweiligen Gerät wichtige, vielleicht sogar geschäftskritische Daten befinden, welche für eine interne Verwendung benötigt wurden. Deshalb ist es wichtig, dass ein Augenmerk nicht nur auf den Schutz der Hardware, sondern auch auf die Sicherung der Daten auf den Systemen liegt.

3.4 Mobile Antivirenprogramme

Diese mobilen Antivirenprogramme schützen das Betriebssystem und die Applikationen des Geräts. Die meisten erkennen bösartige Apps und Seiten, sowie Schadcode. Durch das immer grössere Wachstum an mobilen Endgeräten nimmt das Risiko sich mit solchem Schadcode zu infizieren zu, durch diese Antivirenprogramme kann das Gerät davor geschützt werden.

3.5 Datensicherheit über die Cloud

Cloudbasierte ERP-Systeme stellen eine sichere Alternative zu lokal installierter Unternehmenssoftware dar. Firmendaten werden nach modernster Technik und unter Einhaltung von Hochsicherheitskriterien auf den Servern des Cloud-Anbieters abgelegt. Über Berechtigungen und Zugriffsrechte lässt sich genau regeln, wer was sehen und bearbeiten darf. So sind Daten optimal vor unerlaubten Zugriffen geschützt, und sogar der Diebstahl eines Tablets oder Notebooks kann keinen Schaden anrichten. Zudem entfallen Updates auf den Arbeitsgeräten. Diese implementiert der Cloud-Dienstleister online. Debei sollte aber genau recherchiert werden wie gut der Cloud Anbieter wirklich ist, wie sicher er ist und wie er die Daten verschlüsselt.

3.6 Trennung private und berufliche Daten und Anwendungen

Die strikte Trennung privater von Firmendaten ist ratsam, wenn Mitarbeiter ihr eigenes Smartphone, Tablet oder Notebook im Unternehmensumfeld nutzen. Die Unternehmen sollten jederzeit die Kontrolle über geschäftliche E-Mails,

Dokumente und Applikationen haben, da sie hierfür, insbesondere für personenbezogene Daten, die volle Verantwortung tragen. Denkbar ist die Nutzung unterschiedlicher getrennter Accounts.

Bestimmte Unternehmensdienste lassen sich auch durch spezielle Authentifizierungsmassnahmen schützen. Ebenfalls unerlässlich ist die Vereinbarung, wie mit den Unternehmensdaten auf Privatgeräten verfahren wird, wenn Mitarbeiter die Firma verlassen.

3.7 Kontinuierliche Risikobewertung

Identifizieren und überwachen Sie alle möglichen Anfälligkeiten im Netzwerk und den Geräten. Dies ist keine einmalige Sache, sondern ein konstanter Prozess. Gefahren für die Daten entwickeln sich so schnell, wie sich die Technologie verbessert. Daher sollte eine ständige Überprüfung als Best Practice implementiert werden.

4 Vereinbarungen

Unternehmen müssen im Rahmen eines BYOD-Modells darüber hinaus weitere Punkte regeln, die nur durch zusätzliche Vereinbarungen mit den Mitarbeitern abgedeckt werden können. Dies ist besonders wichtig, da es zum Thema BYOD weder spezifische gesetzliche Regelungen noch eine gesicherte Rechtsprechung gibt.

Um allen Anforderungen gerecht zu werden, müssen Unternehmen ein fachlich und juristisch „sauberes“ BYOD-Modell implementieren, dass auch die entsprechenden Vereinbarungen mit den Mitarbeitern umfasst und eine technische Lösung wählen, die es einfach macht, die rechtlichen Aspekte zu beachten.

4.1 Datensicherheit

Zur Einhaltung der Anforderungen der Datensicherheit müssen sich Mitarbeiter verpflichten, immer ein aktuelles Betriebssystem und aktuellen Virenschutz einzusetzen. Wichtig ist, dass die Mitarbeiter ihre Geräte nicht „jailbreaken“ oder „rooten“ oder an Dritte weitergeben dürfen. Außerdem müssen Regelungen für eine Beendigung der Teilnahme am BYOD-Modell und auch für eine Beendigung des Arbeitsverhältnisses getroffen werden.

4.2 Mitteilungspflicht

Mitarbeiter müssen ihre Unternehmen zeitnah informieren, wenn beispielsweise ein BYOD-Gerät verloren oder gestohlen wurde, damit eine Fernlöschung

vorgenommen werden kann. Ausserdem muss sichergestellt sein, dass etwaige Informationspflichten des Unternehmens nach dem BDSG (Bundesdatenschutzgesetz) erfüllt werden können, wenn Daten unrechtmäßig übermittelt worden sein sollten oder einem Dritten unrechtmäßig zur Kenntnis gelangt sein könnten.

4.3 Haftung

Unternehmen und Mitarbeiter müssen die Haftung bei Verlust oder Beschädigung des Gerätes während der beruflichen Tätigkeit regeln.

4.4 Steuerrechtliche Fragen

BYOD-Geräte unterliegen auch dem Steuerrecht. Hier ist vor allem die Abgrenzung betrieblicher und privater Kosten zu beachten. Übernimmt das Unternehmen Kosten, so muss hier ein geldwerter Vorteil versteuert werden.

4.5 Arbeitsrechtliche Fragen

Wie bei mobilen Geräten, die Arbeitnehmer vom Unternehmen zur Verfügung gestellt bekommen, stellen sich auch bei BYOD arbeitsrechtliche Fragen, die teilweise gerichtlich noch nicht abschließend geklärt sind, beispielsweise hinsichtlich Arbeitszeiten oder ständiger Erreichbarkeit, welche klar ersichtlich und geregelt werden müssen.

5 Vorgehen beim Erstellen einer Police

1. **Risiken aufdecken und informieren:**
   Der erste Schritt für ein erfolgreiches BYOD-Programm ist die Analyse, in welcher Art und Weise Risiken, die durch BYOD entstehen, das Unternehmen beeinträchtigen können. Auch die Mitarbeiter sollten über mögliche Gefahren für ihre persönlichen Daten sowie Unternehmensinformationen aufgeklärt werden.
2. **Expertengruppe einberufen:**
   Für die Implementierung des BYOD-Programms sollten sich die Geschäftsleitung sowie mit den Bereichen IT und Datenschutz zusammenfinden und besprechen wie die bestmögliche Umsetzung aussieht. Auf diese Weise kann das Thema aus verschiedenen Expertenblickwinkeln hinterfragt und effektiv angegangen werden.
3. **Richtlinien festlegen:**
   Eine schriftliche und ordnungsgemäss ausgeführte Vereinbarung zwischen

autorisierten Benutzern und dem Unternehmen ist wichtig. Es ist wichtig, dass die BYOD-Richtlinien sicherstellen, dass die Interessen der Nutzer und der Unternehmen geschützt werden und dafür sorgen, dass alle Rechte und Pflichten klar, prägnant und gesetzlich definiert sind. Welche Regeln sollen für die Nutzung von Mobilgeräten, Tablets und Laptops gelten? Sind die Endgeräte beispielsweise für die Privatnutzung erlaubt? Wenn ja, welche Vereinbarungen gelten bei einem Daten-Screening?

4. **Projektplan erstellen:**
   Der Plan sollte Punkte wie „Remote-Geräteverwaltung“, „Application Control“, „Richtlinienübereinstimmung und Prüfungsberichte“, „Daten- und Geräteverschlüsselung“ sowie insbesondere die „Erhöhung der Sicherheit von Cloud-Storage“ umfassen. Gerade letzteres wird von Sicherheitsexperten als offenstehendes Einfallstor für Hackerangriffe gesehen.

5. **Lösungen implementieren:**
   Zu Beginn des BYOD-Programms sollten verschiedene kleine Testgruppen gebildet werden. Sie setzen sich aus Mitgliedern der Abteilungen zusammen, die auch aus dem Expertenrat bestehen. Anschliessend wird das Programm sukzessive erweitert.

6. **Lösungen neu bewerten:**
   In regelmässigen Abständen sollte in enger Absprache mit Anbietern und Beratern des Vertrauens eine Neubewertung der Lösungen erfolgen. Roadmaps eignen sich in diesem Zusammenhang als wertvolles Instrument für die Evaluierung.

6 Alternativen

6.1 Corporate Owned Personally Enabled (COPE)

Anstatt geschäftliche Funktionen auf privaten Geräten laufen zu lassen, definiert COPE einen Handlungsrahmen zur privaten Nutzung von Firmengeräten. Die Firma wählt bevorzugte Geräte, kauft sie ein, und gestattet den Angestellten, einige persönliche Anwendungen darauf zu installieren und das Gerät auch privat zu nutzen. Als Besitzerin bestimmt die Firma die Benutzungsbedingungen und die Kostenlimite.

6.2 Choose Your Own Device (CYOD)

Bei CYOD werden den Mitarbeitern ein ‚offiziell‘ unterstütztes Gerät (mit oder ohne Kostenbeteiligung der Firma) gekauft und die Firma konfiguriert das Gerät. Änderungen der eingestellten Konfigurationen sind für den Arbeitnehmenden verboten.

6.3 Bring Your Own Connection (BYOC)

Bei BYOC wird ein privates Handy als Hotspot eingesetzt.

6.4 Bring Your Own Software (BYOS)

BYOS beschränkt sich auf portable Anwendungen, die firmenweit einheitlich geregelt werden sollten.

7 Schlusswort

Brind Your Own Device ist ein sehr aktuelles Thema und wird sich in Zukunft sicher noch stark verändern bezüglich der Anwendbarkeit auf verschiedene Gebiete.

Bring Your Own Device kann für alle Beteiligten viele Vorteile bringen, birgt aber auch Risiken. Um diese möglichst gering zu halten, müssen vor Umsetzung dieser Strategie entsprechende Sicherheitsvorkehrungen und klare Regelungen getroffen werden.

???

8 Quellenverzeichnis

https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/arbeitsbereich/bring-your-own-device–byod-.html

http://www.code3pse.com/public/media/22845.pdf

http://www.searchsecurity.de/tipp/BYOD-Policy-Die-fuenf-wichtigsten-Komponenten-fuer-eine-Richtlinie

https://www.computerwoche.de/a/byod-ja-aber-sicher,2517849

9 Anhang

9.1 Beispiel Police

Beispiel Police 1
Beispiel Police 2
Beispiel Police 3

Sample BYOD Policy

This document provides policies, standards, and rules of behavior for the use of personally-owned smart phones and/or tablets by <Department Name> employees to access <Department Name> resources and/or services. Access to and continued use is granted on condition that each user reads, signs, respects, and follows the <Department Name>'s policies concerning the use of these resources and/or services.
This policy is intended to protect the security and integrity of <Department Name>'s data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms.

Expectation of Privacy
<Department Name> will respect the privacy of your personal device and will only request access to the device by technicians to implement security controls or to respond to legitimate discovery requests arising out of administrative, civil, or criminal proceedings. This differs from policy for <Department Name> provided equipment and/or services, where employees do not have the right, nor should they have the expectation, of privacy while using equipment and/or services.

Acceptable Use

- The company defines acceptable business use as activities that directly or indirectly support the business of <Department Name>.
- The company defines acceptable personal use on company time as reasonable and limited personal communication or recreation, such as reading or game playing.
- Devices may not be used at any time to:
    - Store or transmit illicit materials
    - Store or transmit proprietary information
    - Harass others
    - Engage in outside business activities
    - Etc.
- Employees may use their mobile device to access the following company-owned resources:
    - Email
    - Calendars
    - Contacts
    - Documents
    - Etc.
- <Department Name> has a zero-tolerance policy for texting or emailing while driving and only hands-free talking while driving is permitted.

Figure 1: Beispiel Police Seite 1

Devices and Support

- The following devices are supported:
  - iPhone (3GS, 4, 4S, 5, etc…)
  - iPad (<list acceptable models>)
  - Android (<list acceptable models>)
  - Blackberry (<list acceptable models>)
  - Windows (<list acceptable models>)
  - Etc…
- Connectivity issues are supported by IT; employees should contact the device manufacturer or their carrier for operating system or hardware-related issues.
- Devices must be presented to IT for proper job provisioning and configuration of standard apps, such as browsers, office productivity software and security tools, before they can access the network.

Security

- In order to prevent unauthorized access, devices must be password protected using the features of the device and a strong password is required to access the company network.
- The company's strong password policy is: Passwords must be at least six characters and a combination of upper- and lower-case letters, numbers and symbols. Passwords will be rotated every 90 days and the new password can't be one of 15 previous passwords.
- The device must lock itself with a password or PIN if it's idle for five minutes.
- Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network.
- Smartphones and tablets that are not on the company's list of supported devices are not allowed to connect to the network.
- Smartphones and tablets belonging to employees that are for personal use only are not allowed to connect to the network.
- Employees' access to company data is limited based on user profiles defined by IT and automatically enforced.
- The employee's device may be remotely wiped if:
  - The device is lost or stolen.
  - The employee terminates his or her employment.
  - IT detects a data or policy breach, a virus or similar threat to the security of the company's data and technology infrastructure.

Figure 2: Beispiel Police Seite 2

Risks/Liabilities/Disclaimers

- While IT will take every precaution to prevent the employee's personal data from being lost in the event it must remote wipe a device, but it is the employee's responsibility to take additional precautions, such as backing up email, contacts, etc.
- The company reserves the right to disconnect devices or disable services without notification.
- Lost or stolen devices must be reported to the company within 24 hours. Employees are responsible for notifying their mobile carrier immediately upon loss of a device.
- The employee is expected to use his or her devices in an ethical manner at all times and adhere to the company's acceptable use policy as outlined above.
- The employee is personally liable for all costs associated with his or her device.
- The employee assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.
- <Department Name> reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

User Acknowledgment and Agreement

I acknowledge, understand and will comply with the above referenced security policy and rules of behavior, as applicable to my BYOD usage of <Department Name> services. I understand that business use may result in increases to my personal monthly service plan costs. I further understand that reimbursement of any business related data/voice plan usage of my personal device is not provided.

Employee Name: _____

BYOD Device(s): _____

Employee Signature: _____ Date: _____

Figure 3: Beispiel Police Seite 3