Richtlinie
Mobile Endgeräte

Untertitel

Klassifikation:	Bitte klassifizieren!
Datum:	21.02.2019
Version:	0.1a
Autor:	Reiner Schröppel
Dok.-Name:	RL_Mobile Endgeräte_Muster.docx
Seiten:	9

Dokumentenhistorie

Version	Datum	Bearbeiter	Status	Bemerkung/Änderung
0.10	28.11.2018	R. Schröppel	In Bearbeitung	Ersterstellung

Inhaltsverzeichnis

1 Einleitung, Zweck und Ziele

Der Zweck dieses Dokuments ist es, mobile Endgeräte so zu betreiben, dass die auf diesen Geräten gespeicherten Daten nicht durch unbefugte Dritte genutzt werden können bzw. den unberechtigten Zugang zu Mobilgeräten sowohl innerhalb als auch außerhalb den Räumlichkeiten des Unternehmens zu verhindern.

Mobile Endgeräte werden in ständig wechselnden Umgebungen eingesetzt. Sie stellen daher einen der Schnittpunkte zwischen internem Unternehmensnetz und externen Netzen dar. Ein ungenügend geschütztes mobiles Gerät kann damit zur Kompromittierung weiter Teile der Unternehmensinfrastruktur führen.

Grundsätzlich sind folgende Gefährdungen in Zusammenhang mit mobilen Endgeräten denkbar:

- Verlust des mobilen Gerätes
- Verlust der Vertraulichkeit/Integrität von Daten
- Verlust der Integrität von System und Software
- Verlust von Daten
- Identitätsdiebstahl
- Ausspionieren des Unternehmensnetzwerks
- Einschleusen von Schadsoftware in das Unternehmensnetzwerk

Durch Mobilität von Anwendern, spontanen, drahtlosen Netzwerken (ad-hoc Netzwerke) und mobilem

In diesem Umfeld existieren daher zwei grundsätzliche Gefahrenpunkte für Unternehmensnetze und -daten. Zum einen ist das mobile Endgerät und damit gespeicherte Daten und Programme angreifbar, zum anderen besteht die Gefahr für das Unternehmensnetz, dass durch kompromittierte unternehmenseigene Geräte, oder durch missbräuchlich eingesetzte Fremdgeräte das eigene Netzwerk angegriffen und ausspioniert wird.

2 Anwender

Anwender dieses Dokuments sind alle Mitarbeiter innerhalb des Geltungsbereiches des ISMS, die mit mobilen Endgeräten arbeiten, Daten und Informationen auf diesen speichern oder transportieren.

3 Geltungsbereich

4 Definitionen und Begriffe (falls vorhanden)

Begriff	Beschreibung
Apps	Programme (meist für Smartphones), die durch Nutzer selbst installiert werden können. Die Installation geschieht oftmals über sog. „App-Stores“
Geräteverwaltung,	Unter Geräteverwaltung wird im allgemeinen eine Software verstanden, in der mobile Endgeräte erfasst, überwacht und gesteuert werden können. Solche Systeme bieten i. a. Möglichkeiten zur Sperrung, Deaktivierung oder Fernlöschung der Geräte
IrDA	Infrarot-Schnittstelle eines Gerätes, dient meist der Kommunikation od. dem Datenaustasuch
Kensington Schloss	Ein einheitliches System mit dem meist Laptops mittels eines Stahlkabels und einem Schloss gegen Diebstahl gesichert werden können

Begriff	Beschreibung
Mobile Endgeräte	Mobile Endgeräte sind IT-Systeme, die nicht stationär sind. Unter mobilen Endgeräten werden allgemeine tragbare Rechnern (Laptops), Mobiltelefone, Smartphones, oder vergleichbar, verstanden
Mobile Device Management (MDM)	Siehe Geräteverwaltung
NFC	„Near Field Communication“ – eine Schnittstelle um Daten mit anderen Geräten auszutauschen, die sich in sehr kurzem Abstand (meist wenige Zentimeter) zueinander befinden
Personal Firewall	Eine „Personal Firewall“ (PFW) ist ein Programm, welches verhindert, dass ein IT-System über offene Schnittstellen bzw. Ports aus dem Netzwerk angegriffen werden kann. Die PFW blockiert und verhindert diese Zugriffe.

5 Mitgeltende Unterlagen und Referenzdokumente

- Informationssicherheitsleitlinie des Unternehmens
- Klassifizierungsrichtlinie
- Richtlinie zum zulässigen Gebrauch der Unternehmenswerte
- Richtlinie Kryptografie
- ISO/IEC 27001 Standard, Abschnitte

6 Zuständigkeit

Für die Erstellung, Pflege und regelmäßige Überprüfung dieser Richtlinie ist xxx verantwortlich.

7 Umsetzung

7.1 Abgrenzung

Unter mobilen Endgeräten im Sinne dieser Richtlinien werden Geräte verstanden, die über ein Betriebssystem verfügen. Nicht betrachtet werden in dieser Richtlinie Geräte, auf denen Daten transportiert werden können, wie z. B. USB-Sticks, mobile Festplatten, etc.

Da es sich bei den mobilen Endgeräten um Geräte mit unterschiedlichen Einsatzzwecken handelt (Laptops, Tablets, Smartphones) können ggf. nicht alle in dieser Richtlinie gemachten Vorgaben auf jeden gerätetyp angewendet werden. Es ist daher zu prüfen, welche Vorgabe bei welchem Gerätetyp umgesetzt werden kann und welche Vorgabe ggf. in anderer oder vergleichbarer Form bei einem anderen Gerätetyp realisiert werden kann. Diese Richtlinie ist daher als generische Richtlinien zu sehen, die auf alle Gerätetypen anzuwenden ist.

7.2 Grundsätzliches

Nutzern mobiler Endgeräte ist diese Richtlinie zur Kenntnis zu geben und die Kenntnisnahme per Unterschrift zu bestätigen.

Auf mobilen Endgeräten dürfen grundsätzlich nur Daten und Informationen bis zur Sensitivitätsstufe xy

Die Nutzung der mobilen Endgeräten ist ausschließlich zu dienstlichen, bzw. zu dienstlich veranlassten Zwecken gestattet. Für den Fall, dass auf den mobilen Endgeräten private Daten gespeichert werden, ist der

Anwender/Nutzer selbst für diese Daten verantwortlich. Es besteht kein Anspruch, dass die gespeicherten privaten Daten durch das Unternehmen geschützt werden.

Für den Fall, dass auf den Geräten personenbezogenen Daten gespeichert oder verarbeitet werden, ist sicherzustellen, dass diese Daten ausreichend gegen Diebstahl geschützt sind (z. B. durch Verschlüsselung). Der DSB (Datenschutzbeauftragte) ist über die Speicherung (Verarbeitung) zu informieren.

7.3 Benutzerverantwortung

Auf Grund der Tatsache, dass es sich bei mobilen Endgeräten um Geräte handelt, die meist von einem Anwender genutzt werden, und da nicht alle technischen Maßnahmen automatisch greifen können, gibt es grundlegende Tätigkeiten, die durch den Anwender/Nutzer eines mobilen Endgerätes sichergestellt werden müssen.

7.3.1 *Diebstahlschutz*

[redacted]

7.3.2 *Verlust*

Der Verlust oder Diebstahl eines mobilen Endgerätes ist umgehend dem Informationssicherheitsbeauftragten (ISB) und der IT-Abteilung zu melden.

Für den Fall, dass auf dem mobilen Endgerät personenbezogene Daten gespeichert waren (z B. E-Mails, Kundendaten, etc.) ist der Verlust auch dem DSB mitzuteilen.

7.3.3 *Datensicherung*

[redacted]

7.3.4 *Infektion mit Schadsoftware*

Bei Verdacht auf Virenbefall ist das mobile Endgerät nicht mehr mit dem Unternehmensnetz zu verbinden, sondern unverzüglich die IT-Abteilung zu informieren.

7.3.5 *WLAN-Nutzung*

Die Nutzung freier WLANs oder Hotspots ist verboten.

Alternativ: Die Nutzung freier WLANs oder Hotspots ist nur zur Verbindungsaufnahme mittels VPN in das [redacted]

7.3.6 *Nutzung von USB-Ports*

Die Nutzung kostenloser Ladestationen, insbesondere über USB-Anschlüsse, ist verboten. [redacted]

Grundsätzlich ist die Nutzung von USB-Geräten an mobilen Endgeräten untersagt.

7.3.7 *Sonstiges*

Mobile Endgeräte sind so zu schützen, dass diese vor negativen Umwelteinflüssen (Nässe, Hitze, etc.) geschützt sind. Die Geräte sollten daher in entsprechenden Taschen oder Schutzhüllen transportiert werden.

Bei der Nutzung von Smartphones ist bei Gesprächen in der Öffentlichkeit darauf zu achten, dass kein unbefugter Dritter das Gespräch mithören kann. Bei Bedarf ist

Nutzer mobiler Endgeräte sollten darauf achten, dass sie bei der Eingabe von Passwörtern oder PINs nicht beobachtet werden.

7.4 Technische Anforderungen

Die nachfolgenden Anforderungen sind grundsätzlich für alle mobilen Endgeräte anzuwenden, mit denen Daten und Informationen verarbeitet oder auf denen gespeichert werden, sofern dies technisch auf den Geräten möglich ist.

7.4.1 *Sichtschutz*

Mobile Endgeräte, die in der Öffentlichkeit genutzt werden, sind mit einer sog. Sichtschutzfolie zu versehen.

7.4.2 *Verschlüsselung*

Die mobilen Endgeräte sind grundsätzlich mit einem geeignetem Verschlüsselungsverfahren zu verschlüsseln.

Es muss ein Verfahren etabliert und umgesetzt werden, wie auf die verschlüsselten Daten im Falle eines Verlustes eines Passwortes

7.4.3 *Schutz vor Schadsoftware*

Sofern vorhanden und technisch realisierbar, sind Virenschutzmaßnahmen zu implementieren. Es muss dabei sichergestellt werden, dass auch die mobilen Endgerät zeitnah und regelmäßig aktuelle Antivirensignaturen erhalten.

7.4.4 *Patch- und Updatemanagement*

Mobile Endgeräte sind in ein geeignetes Patch- und Updatemanagement einzubinden. Es muss dabei sichergestellt werden, dass auch die mobilen Endgerät zeitnah und regelmäßig aktuelle Patches und Updates erhalten.

7.4.5 *Zugangskontrolle*

Mobile Endgeräte, die längere Zeit (> 2 Wochen) nicht mit dem Unternehmensnetzwerk verbunden waren, müssen, bevor sie sich erneut mit dem Unternehmensnetzwerk verbinden aktualisiert werden (Updates,

7.4.6 *Datensicherung*

Geeignete Datensicherungsmaßnahmen sind vorzusehen, ggf. sind Anwender/Nutzer organisatorisch

7.4.7 *MDM, Mobile Device Management*

Mobile Endgeräte sind mittels einer geeigneten Geräteverwaltung (MDM, Mobile Device Management) zu inventarisieren und zu verwalten.

Die Geräteverwaltung sollte Ortungs- und Fernlöschfunktionen im Falle eines Verlusts oder Diebstahl des

7.4.8 *Passwortschutz, Displaysperre*

Ein mobiles Endgerät muss über ein ausreichendes Passwort bzw. einen ausreichenden Zugriffsschutz verfügen,

7.4.9 *Personal Firewall, WLAN, Hotspots*

Auf mobilen Endgeräten ist eine „Personal Firewall“ zu installieren, sofern das mobile Endgerät diese Funktionalität bietet.

Die Nutzung freier WLANs oder Hotspots ist technisch zu verhindern. Mobile Endgeräte dürfen sich nicht automatisch mit unbekannten oder freien WLAN-Hotspots verbinden.

Alternativ: Nur Geräte, auf denen eine sog. Personal Firewall installiert, konfiguriert und funktionsfähig ist,

Alternativ: Für den Fall, dass ein Gerät als mobiler Hotspot eingesetzt werden soll, dürfen nur

7.4.10 *Sonstige Schnittstellen*

Die Nutzung von [redacted], über die Daten/Informationen übertragen werden können ist zu verhindern, bzw. eine Nutzung restriktiv zu handhaben.

Bluetooth-Verbindung sind nur mit explizit gekoppelten Geräten (Head-Sets, Tastaturen, etc.) zulässig.

[redacted]

7.5 Notwendige Aufzeichnungen

Folgende Aufzeichnungen sind zu führen

- Ausgabe/Rückgabe der mobilen Endgeräte
- Kenntnisnahme dieser Richtlinie
-

8 Freigabe

Ort, Datum	Name in Druckbuchstaben	Unterschrift