Vortrag bei: Deutscher Verein der Blinden und Sehbehinderten in Studium und Beruf e. V.

Datenschutz und Datensicherheit bei der Nutzung privater Endgeräte für berufliche Zwecke

BYOD
„Bring Your Own Device“

Lutz Löscher
Redaktionsbüro & Schulungen
Coach / Dozent vhs Universitätsstadt Marburg

Diese Präsentation unterliegt der Lizenzierung .
Sie darf unter den u.a. Vorgaben an einzelne Personen weitergegeben werden. Öffentliche Vorführungen im Rahmen der Fortbildung sowie Entnahme einzelner Folien sind nicht gestattet.
Andere Verwendungen bedürfen der Erlaubnis des Autors.
LutzLoescher@gmx.de

Zu den folgenden Bedingungen:

Namensnennung — Sie müssen den Namen des Autors/Rechteinhabers in der von ihm festgelegten Weise nennen.

Keine kommerzielle Nutzung — Dieses Werk bzw. dieser Inhalt darf nicht für kommerzielle Zwecke verwendet werden.

Keine Bearbeitung — Dieses Werk bzw. dieser Inhalt darf nicht bearbeitet, abgewandelt oder in anderer Weise verändert werden.

BYOD - Inhalte

Definition	• Private Endgeräte im Unternehmen
Datenschutz	• DSGVO konforme Regelungen
Technik	• Container und Verschlüsselung
Umsetzung	• Konzepte, Richtlinien und Schulungen

Fakten

- Bring Your Own Device – BYOD – ist ein anhaltender und beliebter Trend.

- Im Unternehmensalltag birgt die Nutzung eigener Geräte aber sowohl technische als auch juristische Heraus-forderungen.

Fakten

- Digitale Highend-Technik ist an vielen Arbeitsplätzen keine Selbstverständlichkeit.
- Statt mit veralteter, langsamer Hardware zu arbeiten, bevorzugen viele Angestellte ihre eigenen, oft leistungsstärkeren Geräte.
- „Bring Your Own Device“, kurz BYOD, scheint also eine naheliegende Lösung zu sein.

Fakten

- Private Endgeräte für berufliche Aufgaben zu nutzen, bedeutet für Mitarbeiter vor allem mehr Flexibilität und Wahlfreiheit.
- Gleichzeitig können Unternehmen Kosten für die Anschaffung firmeneigener Hardware sparen.
- Nachteil: es gibt datenschutzrechtliche und technische Risiken.

Datenschutz

- Durch die neue DSGVO sind Unternehmen mehr denn je gefordert, personenbezogene Daten ihrer Mitarbeiter sowie Kunden zu schützen.
- Deswegen muss in Unternehmen ein DSGVO konformes Konzept für BYOD entwickelt werden.
- BYOD erfordert klare Richtlinien und technische Lösungen.

BYOD rechtssicher gestalten

- Verschlüsselung der Daten auf den mobilen Endgeräten.
- Einsatz von Containern = beruflichen und die privaten Daten auf den Smartphones und Tablets werden strikt getrennt.
- Möglichkeit der Fernlöschung bei Verlust

Richtlinien

- Arbeitgeber und Mitarbeiter müssen sich auf folgende Punkte verständigen:
- Mitarbeiter müssen Verschlüsselung, einen Passwortschutz und einen Virenscanner auf den Privatgeräten installieren (lassen).
- Mitarbeiter dürfen berufliche E-Mails nicht an ihr Privatkonto weiterleiten und dürfen keine Daten aus dem Firmennetzwerk herunterladen und speichern.

Container-Ansatz – Prinzipien

- Anstatt das Gerät zu kontrollieren, liegt der Fokus beim Container-Ansatz auf der Sicherung der beruflichen Anwendungen und Daten auf dem mobilen Endgerät.
- Berufliche E-Mails, Kontakte, Kalender, Notizen, Aufgaben und Dokumente kommen in einen verschlüsselten Container.

Container-Ansatz – Beispiele

Die einfachste und sicherste Möglichkeit, mobil zu arbeiten! [720p].mp4 - Verknüpfung.lnk

Container-Ansatz – Beispiele

- die Container-App ist sehr intuitiv, pflegeleicht und absolut unauffällig.
- Dank Office-Integration, integriertem Browser sowie eigener Kamera-App breites Anwendungsfeld.
- Unternehmensdaten werden hochgradig verschlüsselt in einem durch PIN, Passwort oder Fingerabdruck geschützten Sicherheitscontainer abgelegt - separat von privaten Daten.
    - Quelle: https://www.computerwoche.de/a/securepim-office-im-test,3331987

Container-Ansatz – Kostenfrage

- Im Test zeigt sich, dass SecurePIM durchaus geeignet ist, die in vielen Unternehmen noch bestehende Verwaltungslücke für mobile Endgeräte zu schließen.
- Hemmschwelle – die Kosten:
- Virtual Solution verlangt für SecurePIM Office 59 Euro pro Gerät und Jahr

Container-Ansatz – Alternativen

- Mobile Device Management mit Office 365
- Die in MDM for Office 365 enthaltenen Features sollten für die meisten kleineren Unternehmen ausreichen.
- Wer mehr benötigt – Windows INTUNE
- Im Vergleich zu MDM for Office 365 unterstützt Intune zusätzliche Features wie die Verwaltung von Windows-PCs oder Mobile Application Management.

Fazit

- Die hier vorgestellten Lösungen verursachen unterschiedliche Kosten.
- Es sind alles professionelle Lösungen.
- Die Alternative: dienstliche mobile Endgeräte plus Nutzungsvereinbarungen.
- Unabhängig davon wichtig:
- Die Sensibilisierung aller Mitarbeiter für die DSGVO und Infos über die Technik.

Problem: Messenger

- Whatsapp ist praktisch, aber rechtlich heikel: Der Messenger verstößt gegen die Datenschutzgrundverordnung (DSGVO).
- Rund 36.000 Mitarbeiter bei Continental mussten den Messenger vom Diensthandy löschen – aus Datenschutzgründen.
- Auch die Leitung der vhs der Stadt benutzt dienstliche Geräte – und Whatsapp ist TABU

Teamwire -DSGVO konformer Messenger

- **Vorteile**: Teamwire ist ein deutscher Instant-Messenger-Dienst, den vor allem Behörden und Organisationen mit Sicherheitsaufgaben nutzen. Der Dienst, der WhatsApp stark ähnelt, ist für iOS, Android und Windows verfügbar und funktioniert sowohl auf mobilen als auch auf Desktop-Geräten.
- Alle Nachrichten werden verschlüsselt versendet, die Nutzerdaten anonymisiert.
- Adressdaten speichert Teamwire nicht
- Nachrichten speichert die App ausschließlich in deutschen Rechenzentren.

Sicherheitshinweise für mobile internetfähige Geräte:

- Sorgen Sie für einen Basisschutz und führen Sie regelmäßig Sicherheitsupdates durch.
- Installieren Sie Apps nur aus vertrauenswürdigen Quellen und prüfen Sie die Zugriffsberechtigungen.
- Nutzen Sie Sperrcodes und Passwörter.
- Aktivieren Sie Schnittstellen nur bei Bedarf.
- Nutzen Sie öffentliche Hotspots mit erhöhter Vorsicht.
- Quelle: https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/BasisschutzGeraet/EinrichtungMobileGeraete/EinrichtungMobileGeraete_node.html

Sicherheitshinweise für mobile internetfähige Geräte:

- Auch privat ist die Nutzung eines VPN Tunnels sinnvoll und leicht umsetzbar.
- **VPN** steht für “Virtual Private Network” und beschreibt ursprünglich eine Technik, die es Ihnen erlaubt, von jedem Ort auf der Welt sicher auf Ressourcen in Ihrem privaten Netzwerk zuzugreifen. **VPN** verschlüsselt Ihre Internetverbindung beginnend von Ihrer Netzwerkkarte bis hin zu einem **VPN**-Server.

Beispiel VPN Smartphone

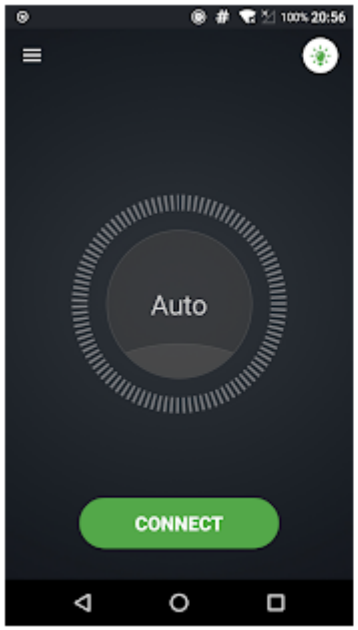
Secure VPN – A high speed, ultra secure VPN

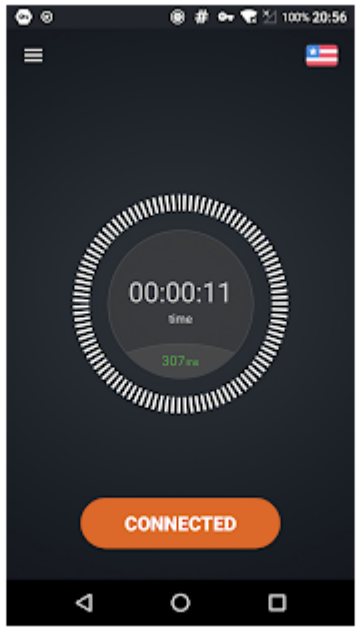
Signal Lab Tools

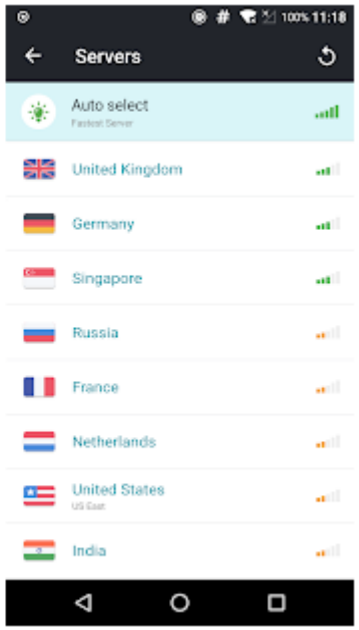
USK: All ages

4.8

5
4
3







Zusammenfassung

- Arbeitgeber: Erstellen Sie eine schriftliche und rechtssichere Vereinbarung zwischen Ihrem Unternehmen und den Mitarbeitern.
- Die Mitarbeiter müssen über sämtliche Gefahren, Rechte und Pflichten aufgeklärt sein.
- Ein Training oder Seminar, in dem alle Richtlinien und Vereinbarungen erklärt werden, hilft weiter.

Beispiel Vereinbarung

Muster-Dienstvereinbarung über die Nutzung privater Smartphones und Tablets für dienstliche Zwecke

Dienstvereinbarung über die Nutzung privater Smartphones und Tablets für dienstliche Zwecke (Bring-Your-Own-Device-Programm – nachfolgend: BYOD-Programm)

Zwischen …

nachfolgend: Dienstgeber

Entwurf-globale-DV-BYOD.pdf - Verknüpfung.lnk

und …

nachfolgend: Mitarbeitervertretung

wird folgende Dienstvereinbarung über die Nutzung privater Smartphones und Tablets für dienstliche Zwecke geschlossen:

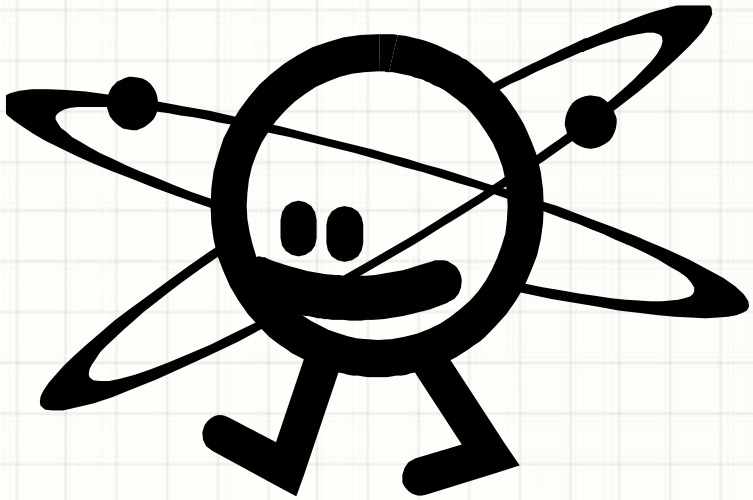
Zum Nachlesen!

Diese Präsentation und andere Materialien stehen Ihnen als PDF zum Download auf meiner Webseite zur Verfügung.

→www.edv-schulung4you.de

Danke für Ihre Aufmerksamkeit!

Viel Erfolg bei
Ihrer Arbeit
wünscht Ihnen
Lutz Löscher…



LutzLoescher@gmx.de
SMS: 015 20 860 40 17