MOBILE UND PRIVATE ENDGERÄTE AM ARBEITSPLATZ

LERNEINHEIT 4

Berufsschüler BOTTOM-UP! für IT-Sicherheit

DIE THEMEN:

1. EINFÜHRUNG: BYOD

2. SICHERHEITSRISIKEN MOBILER ENDGERÄTE

3. SICHERHEITSMASSNAHMEN

> Schutz der Daten auf dem Gerät
> Schutz der Datenverbindungen
> Maßnahmen des Unternehmens
> Trennung von Beruflichem & Privatem
> Interne Richtlinien und Gesetze

1. EINFÜHRUNG: BYOD

Die Nutzung privater Geräte für die Arbeit wird als „**B**ring **Y**our **O**wn **D**evice“ (**BYOD**) bezeichnet: Bring dein eigenes Gerät mit.

HERAUSFORDERUNGEN:

> Mit Schadsoftware infizierte Geräte können die IT im Unternehmen ausspionieren oder Viren weiter übertragen

> Viele verschiedene Mitarbeiter-Geräte bedeuten viele verschiedene Risiken

JEDES EINZELNE GERÄT IST SO GUT WIE MÖGLICH DURCH KENNWORTNUTZUNG, LOKALISIERUNGSSOFTWARE, VERSCHLÜSSELUNG VON DATEN ETC. ZU SCHÜTZEN!

2. SICHERHEITSRISIKEN MOBILER ENDGERÄTE

Leichterer physikalischer Zugriff auf Geräte außerhalb des Büros

Installation vieler Apps auf mobilen Geräten ohne regelmäßiges Sicherheitsupdate

Datenschutz: Auslesen von Informationen, die für die Funktion der App nicht notwendig sind

3. SICHERHEITSMASSNAHMEN

SCHUTZ DER DATEN AUF DEM GERÄT

Betriebssystem und alle Apps aktuell halten	PIN und Bildschirmsperre aktivieren	Dateien auf dem Gerät verschlüsseln/Backups anlegen	Keine sensiblen Daten auf Mobilgeräten speichern
Einstellungen zum Orten/Fernlöschen anpassen	Sicherheits-App installieren	WLAN-Funknetz und Bluetooth deaktivieren	Vorsicht bei der Nutzung öffentlicher WLAN-Hotspots!

VORSORGEMASSNAHMEN TREFFEN!

3. SICHERHEITSMASSNAHMEN

SCHUTZ DER DATENVERBINDUNGEN

GPS, WLAN und Bluetooth nur bei Bedarf einschalten

Nur mit vertrauenswürdigen Netzwerken verbinden

Verschlüsselte Verbindungen verwenden (VPN/SSL)

Zugriffsrechte für Apps auf das Nötigste beschränken

Echtheit des WLAN-Hotspots checken

VORSORGEMASSNAHMEN TREFFEN!

3. SICHERHEITSMASSNAHMEN

MASSNAHMEN DES UNTERNEHMENS

- Beachten der Sicherheitshinweise fördern
- Alle Mitarbeiter*innen zu BYOD-Sicherheitsrisiken schulen
- Liste mit sicheren Apps erstellen
- Nur Original-Geräte und Apps erlauben
- An regelmäßige Backups der Unternehmensdaten erinnern
- Mobile-Device-Management-(MDM)-Software installieren

3. SICHERHEITSMASSNAHMEN

TRENNUNG VON BERUFLICHEM & PRIVATEM

PROFESSIONELLER SCHUTZ – TECHNISCHE MÖGLICHKEITEN

„Container“: eigener geschützter Bereich im Betriebssystem für die Unternehmensdaten und -Apps
Programme und Daten kommen aus der Ferne vom Unternehmen, Bereich ist durch Kennwort geschützt, nur über den gesicherten Bereich kann das Unternehmensnetzwerk erreicht werden

Alternative: Zwei parallel laufende Betriebssysteme
Nicht nur ein geschützter Bereich, sondern ein virtuelles zweites Betriebssystem, Privates und Arbeits-Betriebssystem laufen gleichzeitig, man kann hin und her wechseln

Wenn eine solche Form der technischen Trennung nicht möglich ist:
Nur Web-Anwendungen nutzen, wie z.B. Webmail, Keine Apps oder Daten des Unternehmens auf dem Gerät speichern, Gerät dient nur zur Anzeige von Inhalten, die auf Unternehmensserver liegen

3. SICHERHEITSMASSNAHMEN

INTERNE RICHTLINIEN UND GESETZE I

MÖGLICHKEIT ZUR ÜBERWACHUNG PRIVATER GERÄTE	**MITBESTIMMUNGSRECHT DES BETRIEBSRATS**
PRIVATE E-MAILS UND INHALTE VON MITARBEITERN*INNEN	**ZUGRIFF AUF E-MAILS GRUNDSÄTZLICH VERBOTEN *ABER:* AUFBEWAHRUNGS-PFLICHT BEACHTEN!**
SCHUTZ PERSONENBEZOGENER DATEN DURCH UNTERNEHMEN	**VERHINDERN DES ZUGRIFFS EXTERNER/INFORMATIONS-PFLICHTEN Z.B. BEI VERLUST**

3. SICHERHEITSMASSNAHMEN

INTERNE RICHTLINIEN UND GESETZE II

URHEBERRECHT UND SOFTWARELIZENZEN

Oft ist für privaten Gebrauch kostenlose Anwendungen/Apps für gewerbliche Nutzung kostenpflichtig

Wenn ein Unternehmen den Gebrauch ohne gewerbliche Lizenz duldet, ist es urheberrechtlich haftbar

STEUER- UND HANDELSRECHT

Unternehmen haben bei bestimmten Unterlagen Aufbewahrungs- und Dokumentationspflichten (z.B. bei Rechnungen)

Geschäftsrelevante Unterlagen dürfen nicht gelöscht werden und sollten regelmäßig mit dem Unternehmensserver synchronisiert werden

Berufsschüler BOTTOM-UP! für IT-Sicherheit

Bottom-Up: Berufsschüler für IT-Sicherheit hat zum Ziel, die Mitarbeiter*innen von morgen bereits während der dualen Ausbildung auf die Herausforderungen des digitalen Arbeitsalltags im Hinblick auf IT-Sicherheit und Schutz von Daten vorzubereiten. Damit leistet Bottom-Up einen wichtigen Beitrag zu mehr IT-Sicherheit in kleinen und mittelständischen Unternehmen. **www.dsin-berufsschulen.de**

Bottom-Up: Berufsschüler für IT-Sicherheit ist ein Angebot von
Deutschland sicher im Netz e.V.
Albrechtstraße 10 / 10117 Berlin
www.sicher-im-netz.de

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Im Rahmen der Initiative:
IT-Sicherheit IN DER WIRTSCHAFT

Ein Projekt von:
DsiN Deutschland sicher im Netz

Mit Unterstützung von:
Google

Initiative „IT-Sicherheit in der Wirtschaft“
Die Initiative „IT-Sicherheit in der Wirtschaft“ des Bundesministeriums für Wirtschaft und Energie will vor allem kleine und mittelständische Unter-nehmen beim sicheren Einsatz von IKT-Systemen unterstützen. Gemeinsam mit IT-Sicherheitsexperten aus Wissenschaft, Wirtschaft und Verwaltung soll eine Grundlage dafür geschaffen werden, um die Bewusstseinsbildung in der digitalen Wirtschaft beim Thema IT-Sicherheit im Mittelstand zu stärken. Unternehmen sollen durch konkrete Unterstützungsmaßnahmen dazu befähigt werden, ihre IT-Sicherheit zu verbessern. Weitere Informationen zur Initiative und ihren Angeboten sind unter: **www.it-sicherheit-in-der-wirtschaft.de** abrufbar.