


SCHÜLERMAPPE

SELBSTLERNEINHEIT



MOBILE UND PRIVATE ENDGERÄTE AM ARBEITSPLATZ

LERNEINHEIT 4



LERNEINHEIT 4: MOBILE UND PRIVATE ENDGERÄTE AM ARBEITSPLATZ

Durch Smartphones und Tablets hat man **auch unterwegs immer Zugriff auf Anwendungen (Apps) und seine Daten**. Das schließt auch Anwendungen ein, die man für die Arbeit nutzt: E-Mails, Kalender, Dokumente in der Cloud und vieles mehr. Das ist praktisch und effizient. Aber es stellt auch ein großes **Sicherheitsrisiko** dar, wenn **mobile Endgeräte nicht entsprechend abgesichert werden**, beispielsweise gegen (Daten-)Verlust.



DIE THEMEN:

- | | |
|---|-----------------|
| 1. Sicherheit bei mobilen Endgeräten | Seite 3 |
| 2. (Private) mobile Endgeräte in Unternehmen | Seite 9 |
| 3. Interne Richtlinien und Gesetze: Datenschutz, Lizenzen, Gesetzliches | Seite 12 |
| Übungseinheit | Seite 14 |

*Obwohl aus Gründen der Lesbarkeit im Text die männliche Form gewählt wurde, beziehen sich die Angaben auf Angehörige aller Geschlechter.



1. SICHERHEIT BEI MOBILEN ENDGERÄTEN

Mobile Sicherheit nicht flächendeckend vorhanden

Laut **DsiN-Sicherheitsmonitor Mittelstand 2016** haben rund drei Viertel der KMU keine Sicherheitsmaßnahmen gegen die Gefahren im Umgang mobiler Endgeräte ergriffen, bzw. sind sich nicht sicher, ob die vorhandenen Maßnahmen ausreichend sind. In vielen Unternehmen kann dies zu einer **Sicherheitsproblematik** führen. Diesem Umstand kann die IT nur mit der Umsetzung einer nachhaltigen **Sicherheitsstrategie** und der Einführung einer Lösung im Bereich **Mobile Device Management** (siehe unten) begegnen.



LINKTIPP

Hier geht es zur DsiN-Studie Sicherheitsmonitor Mittelstand 2016:
https://www.sicher-im-netz.de/sites/default/files/download/dsin_sicherheitsmonitor_2016_web.pdf

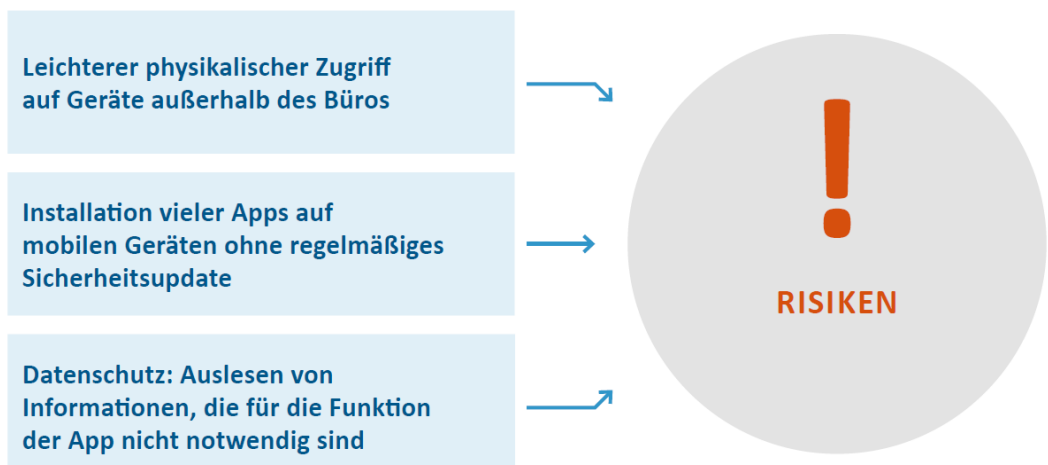
Apps von Drittanbietern können Sicherheitsrisiko bedeuten

Unsichere Apps können Kennwörter, Telefonnummern etc. ausspähen und an Dritte übertragen.

Auf Smartphones und Tablets lassen sich neben den Apps, die mit dem Betriebssystem kommen (zum Beispiel das Kontaktverzeichnis), **unzählige Apps von Drittanbietern aus unterschiedlichen App-Stores installieren**. Aufgrund niedriger Sicherheitsstandards vieler Drittanbieter-Apps können sich **Sicherheitslücken** einschleichen – oder absichtlich eingebaut werden. Über **unsichere Apps** können **Unbekannte** Schadsoftware auf Smartphones aufspielen und **sensible Daten ausspähen oder manipulieren**. Zu diesen Daten zählen insbesondere Kennwörter, Telefonnummern, Anruflisten, Nachrichten, Fotos etc.

Zugriffsrechte der Apps kontrollieren.

Viele Apps sammeln ausgiebig Daten - obwohl sie sie für das Ausführen der eigentlichen Funktion nicht benötigen. Dazu gehören oftmals Kontaktdaten und Aufenthaltsorte. Die meisten Smartphone-Betriebssysteme erlauben es, die Zugriffsrechte für Apps anzupassen. **Apps sollten nur die Zugriffsrechte erhalten, die für die Ausführung der Funktionen der App auch notwendig sind**. Außerdem kann man vor der Installation bereits prüfen, welche Zugriffe eine App verlangt.





SICHERHEITS-APP

Eine Sicherheits-App installieren und diese regelmäßig aktualisieren. Manche der Apps überprüfen neben einem laufenden Schutz des Endgerätes zusätzlich, auf welche Daten und Bereiche des Geräts installierte Apps zugreifen können. Zu den Funktionen der Sicherheits-Apps gehören auch eine Kindersicherung und die Möglichkeit, Anrufe und SMS-Nachrichten zu blockieren.

Das mobile Betriebssystem sollte **immer aktuell gehalten werden**. Mit den Updates schließen die Hersteller bekannte Sicherheitslücken!



ANREGUNG

Überlegen Sie: Welche Sicherheitsvorkehrungen für mobile Endgeräte sind ratsam?

Mindestmaß an Schutz mobiler Geräte mithilfe von grundlegenden Einstellungen:

- ✓ PIN
- ✓ Bildschirmsperre
- ✓ Verschlüsselung des Speichers

Bildschirmsperre aktivieren

Die Bildschirmsperre auf dem Smartphone und Tablet **sollte immer aktiviert sein**. Ansonsten haben Unbekannte sofort Zugriff auf die Daten und Funktionen, sobald sie das Gerät in die Hände bekommen. Die Bildschirmsperre kann auf den meisten Geräten durch eine **PIN** („Persönliche Identifikationsnummer“) oder eine **Mustersperre** eingerichtet werden. Bei der Mustersperre kann man ein eigenes Muster aus verschiedenen vorgegebenen Punkten zusammensetzen, z.B. ein Rechteck, Quadrat oder einen Buchstaben. Auf dem Touch-Display entstehen im Laufe der Zeit sichtbare **Spuren durch Fingerabdrücke**, die regelmäßig entfernt werden sollten. Neuere Geräte kann man auch mit einem Fingerabdruckscanner entsperren.



DAS GERÄT SPERREN

Auf Nummer sicher gehen und Bildschirmsperre aktivieren. Zum Entsperren sollte ein ausreichend komplexer Zugangscode oder gleich ein Passwort verwendet werden. Kombinationen wie 1234 oder 3333 sind nicht sicher! Auf jeden Fall sollte der Entsperrungscode – wenn möglich – aus mehr als vier Zahlen bestehen.

Außerdem sollte man die SIM-Karte schützen, indem jedes Mal, wenn das Gerät aus- und wieder eingeschaltet wird, zum Entsperren aufgefordert wird.



Verschlüsselung der Daten

Um die Daten zusätzlich abzusichern, sollten **sie auf dem Gerät verschlüsselt** werden. Diese Funktion ist in den meisten neueren Betriebssystemen eingebaut und kann in den Einstellungen des Geräts aktiviert werden. Besonders bei Geräten, die auch für betriebliche Zwecke eingesetzt werden und damit Firmendaten speichern, ist dies ratsam. (**Achtung:** vergisst der Nutzer das Passwort für die Entschlüsselung, werden die Daten unbrauchbar, da sie nicht mehr lesbar sind. Von Sicherungskopien unverschlüsselter Daten ist bei Unternehmen dennoch abzuraten. Schauen Sie hier auch die **Lerneinheit 3 – Datensicherung & Notfallplanung.**)

Verlust des Gerätes

Die IMEI-Nummer befindet sich an den Geräten oder auf der Originalverpackung.

Wird ein mobiles Gerät gestohlen oder geht verloren, ist es wichtig schnell zu handeln. Beim **Netzbetreiber** kann man die **SIM-Karte sperren lassen**, um mobile Datenverbindungen und Telefonate über das verlorene Gerät zu unterbinden. Bei einem Diebstahl sollte außerdem **Anzeige bei der Polizei** erstatten werden – besonders, wenn es sich um Firmengeräte handelt. Jedes Smartphone hat eine **IMEI-Nummer**, über die es identifiziert und in manchen Fällen auch gesperrt werden kann.

Die Nummer findet sich unter dem Akku, auf der Originalverpackung oder der Rechnung. Die IMEI-Nummer sollte an einem sicheren Ort aufbewahrt und im Ernstfall der Polizei mitgeteilt werden. Für den Fall des Verlusts ist es ratsam, im Voraus eine **Sicherheits-App** zu installieren, mit der das **Gerät lokalisiert** werden kann. Auf manchen Smartphones ist diese Funktion schon im Betriebssystem vorgesehen. Damit kann man oft auch die Daten auf dem Gerät **aus der Ferne löschen**.

Das Orten des Gerätes über diese Apps funktioniert oftmals nur solange, wie GPS eingeschaltet ist. Möchte man GPS und andere Ortungsdienste nicht dauerhaft einschalten (siehe unten „Standortdaten kontrollieren“), bieten sich Apps an, die das Gerät über das **Mobilfunknetz** orten (die Genauigkeit der Lokalisierung ist hierbei allerdings geringer als über GPS). Aber Achtung: Diese Methode funktioniert in der Regel nur solange, wie das Gerät eingeschaltet ist und die SIM-Karte nicht entfernt oder gesperrt wurde. Es gibt Sicherheits-Apps, die dem Eigentümer nach dem Austausch der SIM-Karte automatisch die Nummer der neu eingesetzten SIM-Karte per SMS schicken. Eine Fernlöschung ist auch dann noch möglich.



LINKTIPP

Auf der Webseite <https://mobilsicher.de> gibt es viele nützliche Hinweise, wie man sein Gerät schützen kann (für verschiedene Gerätehersteller). Es gibt Anleitungen für die datensparsame Einrichtung des Geräts und Erste-Hilfe-Tipps bei Verlust und Diebstahl.



Sichere WLAN Verbindungen

Um vertrauliche Informationen zu schützen, sollte **nie eine ungesicherte Verbindung mit ungeschützten WLAN-Netzen** hergestellt werden. Sichere Netze sind mit dem **WPA2-Standard** verschlüsselt und verlangen bei der Verbindung die **Eingabe eines Passworts**.



ANREGUNG

Überlegen Sie: Was könnten Risiken bei der Nutzung eines öffentlichen WLAN-Netzwerks sein?

Achtung ist geboten bei der Übertragung sensibler Daten über öffentliche WLAN-Hotspots!

Öffentliche WLAN-Hotspots sind oft ungesichert. Die gesamte Kommunikation zwischen den Geräten und dem Router (der den Internetzugang herstellt) kann von Dritten mit der richtigen Ausrüstung mitgelesen werden. WLAN-Router mit einer vertrauenswürdigen SSID (Netzwerkname) können von Angreifern nahe einem „echten“ Hotspot platziert werden, um dessen Verbindungen zu „**kapern**“. Vor allem bei Hotspots mit SSID-Namen wie „**freies WLAN**“ oder ähnlich gut klingenden Angeboten sollte erhöhte **Vorsicht** geboten sein. Wenn dann die Zugangsdaten und andere vertrauliche Informationen ohne Wissen des Nutzers an den falschen WLAN-Router übermittelt werden, fallen diese in die Hände des Angreifers.

Im Vergleich zu firmeninternen Netzwerken kann der Nutzer bei öffentlichen Netzwerken grundsätzlich keine Aussagen über deren Sicherheit treffen: wurde der WLAN-Router vom Betreiber ausreichend gegen Angriffe abgesichert? Wurden aktuelle Firmwareupdates aufgespielt und so mögliche Sicherheitslücken geschlossen? Daher sollten im Normalfall **über ein öffentliches und möglicherweise ungesichertes WLAN gar keine sensiblen Firmendaten** übertragen werden. Dazu zählt bereits das Abrufen von E-Mails. Derartige Daten sollten im besten Fall nur über das **Mobilfunknetz** angefordert werden.

Vorsicht bei Netzwerken mit der SSID „freies WLAN“!

Grundsätzlich ist in den Einstellungen des eigenen Gerätes zu empfehlen, dass es sich **nicht automatisch mit jedem verfügbaren WLAN verbindet**. Die Verbindung sollte stets manuell und mit Bedacht gewählt werden.



ACHTUNG

Alle angegebenen Zugangsdaten können von anderen mitgehört und missbräuchlich verwendet werden, sollte der Hotspot-Betreiber keinen verschlüsselten WLAN-Zugang anbieten.



So erkennen sie eine verschlüsselte Verbindung in der Adresszeile des Browsers:



Die **Anmeldung an einem WLAN-Hotspot erfolgt im besten Fall per Benutzername und Passwort**. Diese erhält man vom Betreiber des Hotspots. Die Zugangsdaten sind bei der Anmeldung über eine verschlüsselte Verbindung zu übertragen, damit sie nicht bereits hier abgehört werden können. Diese Verbindung erkennt man am „**https://**“ in der Adresszeile und dem eingblendeten Schlosssymbol (siehe links).

Häufig wird eine Verschlüsselung aber nur für den **Anmeldevorgang** eingesetzt. Nach der Anmeldung wird im Anschluss unverschlüsselt im Internet gesurft. In diesem Fall – wie eigentlich immer – bietet sich an, eine Verbindung zu bestimmten Diensten wie Online-Banking, E-Mail, etc. ausschließlich über eine **TLS/SSL-Verschlüsselung** herzustellen. Hier ist es ratsam, mit Bookmarks zu den gewollten Webseiten zu arbeiten, bevor man über einen Tippfehler bei der Adresseingabe im Browser oder Links zu einer gefälschten Seite geführt wird. Es sollten auch keine in E-Mails oder auf Webseiten propagierten Links geklickt werden, auch die können auf eine gefälschte Seite führen.

(Viele Websites bieten eine verschlüsselte Verbindung übrigens an, stellen diese aber nicht standardmäßig her. Der Nutzer muss also jeweils in der Adresszeile **https://** vor dem Domainnamen eingeben, um auf die verschlüsselte Version der Website zu gelangen. Browser-Erweiterungen wie HTTPS EVERYWHERE übernehmen diese Aufgabe für den Nutzer automatisch.)



ACHTUNG

Geräte nur mit gesicherten Netzwerken verbinden, denen man vertraut!

Um die Datenverbindungen innerhalb eines WLAN-Netzes zu verschlüsseln, das von Unbekannten mitbenutzt wird, kann eine **VPN-App** genutzt werden. VPN steht für **Virtuelles Privates Netzwerk** und bietet eine zusätzliche Ebene der Sicherheit. Je nach Anbieter muss hierfür eine zusätzliche App auf dem Smartphone installiert werden.



LINKTIPP

Die **SiBa-App** von DsiN informiert über neueste Bedrohungen durch Schadsoftware, auch auf mobilen Geräten:

<https://www.sicher-im-netz.de/siba>



Standortdaten kontrollieren

Es ist möglich, über die Funktion der **GPS-Standortbestimmung** und anhand der Mobilfunkzellen, mit denen sich ein Gerät verbindet, **Bewegungsprofile des Geräteinhabers** zu erstellen. Das Gleiche gilt für **dauerhaft aktivierte WLAN- und Bluetooth-Verbindungen**, weil das Gerät dann durchgehend nach vorhandenen WLAN-Netzen sucht.

Bewegungsprofile des Handybesitzers können angelegt werden.

✓ GPS-Standortdaten deaktivieren

GPS-Daten liefern Anwendungen Informationen über den aktuellen Standort oder auch Bewegungsprofile. Für ein Unternehmen kann es unter Umständen gefährlich sein, z.B. wann ein Mitarbeiter (möglicherweise der letzte im täglichen Betrieb) das Büro verlässt, so dass im Anschluss daran ein Einbruch durchgeführt werden könnte.

✓ Andere Standortdaten deaktivieren

Auch ohne GPS kann der Standort mobiler Geräte bestimmt werden. Smartphones können anhand der Mobilfunknetze, in denen sie sich befinden, lokalisiert werden. Anhand der Signalstärken ist eine Lokalisierung bis auf wenige hundert Meter des Gerätes möglich.

✓ WLAN-Funknetz und Bluetooth deaktivieren

WLAN und Bluetooth sollten nur bei Bedarf aktiviert werden, um eine unfreiwillige Weitergabe des eigenen Standorts zu verhindern. Beide Schnittstellen können unter Umständen von Angreifern ausgenutzt werden – ganz ohne Wissen des Nutzers. Die Benutzererkennung über Bluetooth sollte nur bei Bedarf übertragen werden (Benutzererkennung in den Einstellungen „verbergen/verstecken“). Damit kann sich ein anderer Nutzer mit dem Gerät nur verbinden, wenn er den Benutzernamen kennt, und dessen Verbindungsanfrage der Besitzer erst bestätigen muss. Den Gerätetypen sollte die Benutzererkennung auf keinen Fall übertragen.

GPS, WLAN, Bluetooth und weitere Standortdienste nur nach Bedarf einschalten.

In allen Fällen sollten Unternehmen bzw. ihre Mitarbeiter **genau abwägen**, wann eine Aktivierung der Standortdaten in Betracht gezogen werden soll. Manche Lokalisierungsdienste zum Auffinden verlorener oder gestohlener Geräte greifen beispielsweise auf GPS Daten zurück (siehe oben).

VORSORGEMASSNAHMEN TREFFEN!





2. (PRIVATE) MOBILE ENDGERÄTE IM UNTERNEHMEN

Viele Unternehmen stellen ihren Mitarbeitern mobile Endgeräte für die Arbeit zur Verfügung. Eine Alternative ist die Einführung von **BYOD** („Bring your own Device“): **Bring dein eigenes Gerät mit** – und nutze es gleichzeitig für die Arbeit.



ANREGUNG

Überlegen Sie: Nutzen Sie ein privates Gerät bei der Arbeit? Was sind die Vor- und Nachteile von BYOD?

Unsichere Geräte können zum Ausspähen und Diebstahl betriebsinterner Daten führen.

Ein Problem bei der Nutzung von BYOD ist, dass **viele Unternehmen keine angepasste Sicherheitsstrategie haben**. Oft werden die IT-Verantwortlichen nicht darüber informiert, welche Geräte mitgebracht und verbunden werden oder welche Software die Mitarbeiter installieren (das wird auch als „**Schatten-IT**“ bezeichnet). Unsichere Geräte können die IT im Unternehmen gefährden, zum Beispiel durch Ausspähen und Diebstahl von Daten und Informationen oder durch die Übertragung von Schadsoftware.

Deshalb ist es wichtig, dass die Mitarbeiter besonders auf die Sicherheit ihrer eigenen Geräte achten. Die Mitarbeiter können aber noch mehr tun: Sie können Kollegen darauf ansprechen, **ob es im Unternehmen bereits eine Richtlinie für den Umgang mit BYOD gibt**, und gegebenenfalls vorschlagen, eine solche aufzustellen.

Wichtig ist dabei, dass alle Mitarbeiter die erstellten **Sicherheitshinweise** beachten. **Regelmäßige Schulungen** können dabei sinnvoll sein. Die IT-Abteilung kann zudem eine **Positivliste** erstellen, welche Apps ohne größere Bedenken vom Nutzer installiert und benutzt werden können.

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, VERSCHLÜSSLUNG VON DATEN ETC. ZU SCHÜTZEN!



Mobile-Device-Management

Um die **Sicherheit von privaten Geräten zu erhöhen**, kann die IT-Abteilung des Unternehmens spezielle MDM-Software (**Mobile-Device-Management**) installieren, die bei allen Mitarbeiter-Geräten gewisse Funktionen bereitstellt: verschlüsselte Verbindungen (zum Beispiel über ein VPN), eine Firewall, eine zwingende PIN-Eingabe, die Fernlöschung von Daten bei Verlust und einiges mehr.

Durch eine **softwarebasierte Trennung der Unternehmensdaten von privaten Apps und Daten** kann mit MDM-Software zudem ein **professioneller Schutz** erreicht werden. Die Trennung stellt sicher, dass unsichere Apps, die auf dem Gerät installiert sind, nicht auf Systembereiche zugreifen können, die der Arbeit vorbehalten sind. Hier gibt es verschiedene Möglichkeiten.

Optimal ist die Trennung des privaten und des beruflichen Bereichs eines mobilen Endgerätes.

- ✓ „**Container**“: Auf dem Gerät wird ein **geschützter Bereich**, ein sogenannter Container, eingerichtet, der vom Unternehmen aus der Ferne mit Programmen und Daten versehen werden kann. Der Bereich ist durch ein **Kennwort** geschützt. Nur über den gesicherten Bereich kann das Unternehmensnetzwerk erreicht werden.
- ✓ Es ist auch möglich, ein **komplettes zweites Betriebssystem** einzurichten. Dieses kann gleichzeitig mit dem privat genutzten Betriebssystem ausgeführt werden und es kann während der Benutzung des Geräts jederzeit hin- und her gewechselt werden

Sollte eine Trennung technisch nicht umsetzbar sein, gibt es die Möglichkeit, auf privaten Geräten **nur Web-Anwendungen** zu nutzen, wie zum Beispiel Webmail. **In dem Fall gibt es auf dem Gerät keine Anwendungen oder Daten des Unternehmens.** Es dient nur zum Anzeigen von Inhalten, die auf dem Server des Unternehmens liegen und nicht auf dem Gerät gespeichert werden. Hier gibt es **Software, die webbasiert umfangreiche Funktionen** bereitstellt.



ANREGUNG

Überlegen Sie: Gibt es in Ihrem Ausbildungsbetrieb eine Richtlinie für den Umgang mit BYOD? Wird eine Mobile-Device-Management Software genutzt?



BACKUPS

Bei Geräten mit Geschäftsdaten sind regelmäßige Backups der Daten ratsam (auf einer Festplatte oder in einer geschützten Cloud). Hier sind feste Termine eine nützliche Gedächtnisstütze. Kollegen können sich zudem gegenseitig daran erinnern.

Jailbreaking und **Rooting**: zusätzliches Sicherheitsrisiko.

Vor allem für mobile Geräte gilt: Aus Sicherheitsgründen sollten keine Geräte verwendet werden, deren Betriebssystem verändert wurde (zum Beispiel durch „**Jailbreak**“ oder „**Rooting**“ - mit denen ein Anwender durch administrativen Zugang zum Betriebssystem versucht, beliebige Software zu installieren. Dadurch kann der Zugang von Schad- und Malware begünstigt werden, weil durch den Eingriff die Schutzmechanismen des Systems oftmals abgeschaltet werden.)



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. INTERNE RICHTLINIEN UND GESETZE: DATENSCHUTZ, LIZENZEN, RECHTLICHES

Die Verwendung von privaten Geräten bei der Arbeit bringt für die Unternehmen bestimmte **rechtliche Verpflichtungen** mit sich. Um diese zu erfüllen, ist die **Hilfe der Mitarbeiter wichtig**.

Datenschutz

Unternehmen müssen bei BYOD eigene Richtlinien dem Datenschutz entsprechend ausrichten.

Durch Einbindung in die Unternehmens-IT könnten **private Geräte überwacht werden**. Der **Betriebsrat hat deshalb ein Mitbestimmungsrecht bei der Einführung von internen BYOD-Richtlinien**. Mitarbeiter können nicht gegen ihren Willen gezwungen werden, Software auf ihren privaten Geräten zu installieren, die es ermöglicht, ihr Verhalten zu überwachen.

Bei privaten Mails und Inhalten von Mitarbeitern gilt das Fernmeldegeheimnis. Unternehmen dürfen diese nicht einsehen. Selbst wenn ein Unternehmen technisch die Möglichkeit hätte, auf private Mails von Mitarbeitern zuzugreifen, zum Beispiel mit einer MDM-Software, die auf einem (privaten) mobilen Gerät installiert ist, darf es dies nicht tun. Mitarbeiter sind durch das Gesetz vor solchen Zugriffen geschützt.

Unternehmen müssen personenbezogene Daten schützen. Externe dürfen keinen Zugriff auf Geräte mit personenbezogenen Daten (z.B. von Kunden) bekommen. Das gilt auch für Familienmitglieder von Angestellten. So lange Kundendaten auf dem Gerät sind, kommen kein Verkauf und keine Reparatur durch externe Dienstleister in Frage. Wenn einem Mitarbeiter ein Gerät mit personenbezogenen Daten von Dritten verloren geht, muss das Unternehmen benachrichtigt werden, um es der zuständigen Datenschutzaufsichtsbehörde zu melden. Dazu sind alle Unternehmen gesetzlich verpflichtet, die personenbezogene Daten verarbeiten.





ANREGUNG

Überlegen Sie: Hat ihr Ausbildungsbetrieb die private Nutzung von Geräten und Firmenmails geregelt? Gibt es diesbezüglich bereits Erfahrungen?

Urheberrecht und Softwarelizenzen

Viele Apps sind **kostenlos, wenn man sie privat nutzt**, müssen aber für **gewerbliche Nutzung bezahlt** werden. Verwenden Mitarbeiter solche Apps auch bei der Arbeit, muss das **Unternehmen informiert** werden, damit die nötigen Lizenzen erworben werden können. Ansonsten kann das Unternehmen **haftbar gemacht werden**. Das gilt gleichermaßen für Apps auf privaten Tablets und Smartphones (zum Beispiel bei der mobilen Version einer Office-Anwendung) wie auch für Programme auf privaten Laptops, auf denen der Nutzer Aufgaben für die Firma erledigt.

Steuer- und Handelsrecht

Unternehmen sind verpflichtet, bestimmte Unterlagen wie zum Beispiel Rechnungen aufzubewahren und zu dokumentieren (das wird auch **Aufbewahrungs- und Dokumentationspflicht** genannt). Solche Unterlagen **dürfen nicht gelöscht werden**, auch nicht wenn sie auf privaten Geräten entstehen. Geschäftsrelevante Unterlagen sollten deshalb nicht allein auf dem eigenen Gerät gespeichert, sondern auch **regelmäßig mit dem Unternehmensserver synchronisiert** werden. Wenn zum Beispiel ein Unternehmen unter Zeitdruck einer Medienagentur einen Auftrag vergibt, indem ein Mitarbeiter eine Datei über eine Messaging-App auf dem privaten Smartphone schickt, muss diese Datei entsprechend gesichert aufbewahrt werden.



LINK-TIPP

Ausführliche Informationen zu rechtlichen und technischen Herausforderungen der Nutzung von privaten Geräten im Unternehmen finden sich im Leitfaden „Bring your own Device“ des Verbandes BITKOM von 2013: <http://t1p.de/w88s>



QUIZ Q4



Sie können das folgende Quiz alternativ auch in Form eines Online-Spiels direkt auf Ihrem Smartphone oder Computer durchführen.

Das Online-Quiz ist verfügbar auf der Bottom-Up-Webseite:
<https://www.dsin-berufsschulen.de/unsere-online-quiz>.

1. Warum sammeln viele Apps heimlich Informationen über die Nutzer?

- A Weil die App-Entwickler*innen besonders neugierige Nerds sind.
- B Weil eine App, die kaum Daten erhebt, langweilig zu programmieren ist.
- C Um anhand der Nutzerdaten zum Beispiel gezielte Werbung einzuspielen.

2. Warum ist es gefährlich, wenn ein Gerät nicht durch eine Bildschirmsperre geschützt ist?

- A Jeder, der das Gerät in die Hände bekommt, kann auf die gespeicherten Daten zugreifen.
- B Hacker könnten über die Kamerafunktion meinen Gesprächen lauschen.
- C Weil sich das Gerät sonst ungehindert mit einem WLAN-Hotspot verbindet.

3. Was sollte man bei Verlust des Geräts bezüglich der SIM-Karte tun?

- A Nichts, die ist ja im Gerät.
- B Man sollte sie vom Netzbetreiber sperren lassen.
- C Man kauft sich einfach eine neue Karte. Die Telefonnummer ist ja auf den eigenen Namen angemeldet.

4. Warum sollte die WLAN-Funktion nur bei Bedarf eingeschaltet werden?

- A Weil sich das Gerät sonst versehentlich mit fremden Netzwerken verbinden könnte und deren Datenvolumen mit verbrauchen würde.
- B Weil die Frequenz überlastet wäre, wenn jeder die ganze Zeit seine WLAN-Funktion aktiviert hätte.
- C Aus Datenschutz-Gründen: die WLAN-Funktion kann auch dafür verwendet werden, Bewegungsprofile zu erstellen.

5. Warum ist BYOD eine Herausforderung für die IT-Sicherheit eines Unternehmens?

- A Weil die IT-Verantwortlichen keine Zeit haben, den Mitarbeiter*innen zu helfen, wenn sie privat unterwegs sind.
- B Weil dadurch viele verschiedene Geräte mit verschiedener Software mit dem Unternehmens-Netzwerk verbunden werden.
- C Weil BYOD ein Verfahren aus der Schatten-IT ist, und das ist illegal.



- 6. Was ist bei einer internen BYOD-Richtlinie für das Unternehmen besonders wichtig?**
- A Dass die Richtlinie geheim bleibt. Wenn zum Beispiel die Konkurrenz die Richtlinie kennt, sind Geschäftsgeheimnisse in Gefahr.
 - B Dass jede*r Mitarbeiter*in ein Mitspracherecht bei der Aufstellung der Regeln hat. Mitarbeiter*innen müssen bei allen IT-Entscheidungen vorher gefragt werden.
 - C Dass sich alle Mitarbeiter*innen an die Regeln halten. Schon ein einzelnes unsicheres Gerät ist ein Risiko für das Unternehmen.
- 7. Auf einem privaten mobilen Endgerät befinden sich Kundendaten des Unternehmens. Wer darf darauf zugreifen?**
- A Nur der/die Mitarbeiter*in, dem das Gerät gehört und eventuell ein Dienstleister, der das Gerät repariert, wenn es kaputt ist.
 - B Nur der/die Mitarbeiter*in, dem das Gerät gehört und eventuell andere Mitarbeiter*innen des Unternehmens.
 - C Nur der/die Mitarbeiter*in, dem das Gerät gehört und seine Familienmitglieder, wenn sie das Gerät nur für private Zwecke nutzen.
- 8. Kann ich als Mitarbeiter*in ein mobiles Endgerät bei der Arbeit genauso nutzen wie privat?**
- A Nein, manche Apps sind privat kostenlos, kosten für Unternehmen aber Geld. Das muss für jede App überprüft werden.
 - B Nein, Unterhaltungs-Apps sind bei der Arbeit generell verboten. Das Abspielen von Videodateien führt zum Beispiel fast immer zur Kündigung.
 - C Ja, das ist ja die Idee von BYOD – Mitarbeiter*innen sollen stets erreichbar sein.

Lösung: 1 C, 2 A, 3 B, 4 C, 5 B, 6 C, 7 B, 8 A



BOTTOM-UP: BERUFSSCHÜLER FÜR IT-SICHERHEIT

hat zum Ziel, die Mitarbeiter 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 mittleren Unternehmen.

www.dsin-berufsschulen.de

Bottom-Up ist ein Angebot von

Deutschland sicher im Netz e.V.
Albrechtstraße 10
10117 Berlin

www.sicher-im-netz.de

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

Im Rahmen der Initiative:



Ein Projekt von:



Initiative „IT-Sicherheit in der Wirtschaft“ Die Initiative „IT-Sicherheit in der Wirtschaft“ des Bundesministeriums für Wirtschaft und Energie will vor allem kleine und mittlere Unternehmen 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.