LEHRERMAPPE

LESESKRIPT & UNTERRICHTSMATERIAL

Berufsschüler BOTTOM-UP! für IT-Sicherheit

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:

Für welche Ausbildungslehrgänge empfohlen?

Diese Lerneinheit wird **Ausbildungslehrgangsübergreifend** und vor allem bei fehlendem Grundlagenwissen empfohlen. Für **handwerklich/praktisch orientierte Ausbildungslehrgänge** bietet sich insbesondere das erste und - mit Abstrichen - das dritte Kapitel an.

LERNZIELE

Nach diesen Unterrichtseinheiten wissen die Schüler*:

- ✓ wie sie mobile Geräte möglichst sicher verwenden,
- ✓ was sie bei der Nutzung von Netzwerken und Verbindungen beachten sollten,
- ✓ was sie zusätzlich beachten müssen, wenn sie ihr Gerät beruflich nutzen,
- ✓ was getan werden muss, um das Unternehmen vor Risiken zu schützen.

*Obwohl aus Gründen der Lesbarkeit im Text die männliche Form gewählt wurde, beziehen sich die Angaben auf Angehörige aller Geschlechter. In den Arbeitsmaterialien für den Unterricht wird dagegen das Gender-Sternchen verwendet.

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

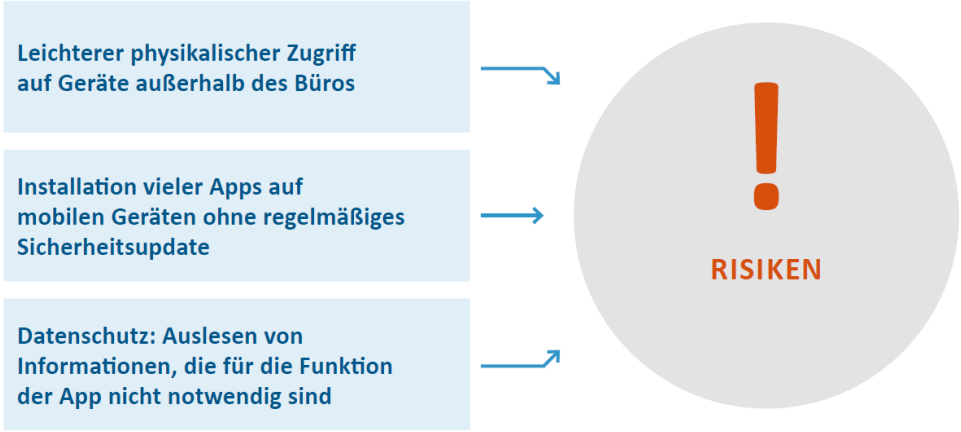
Apps von Drittanbietern können Sicherheitsrisiko bedeuten

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 FÜR DEN UNTERRICHT

Diskussionsfragen: Welche Sicherheitsvorkehrungen für mobile Endgeräte sind ratsam?

Bildschirmsperre aktivieren

Mindestmaß an Schutz mobiler Gerät mithilfe von grundlegenden Einstellungen:
- ✓ PIN
- ✓ Bildschirmsperre
- ✓ Verschlüsselung des Speichers

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 FÜR DEN UNTERRICHT

Diskussionsfragen: 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 eingeblendeten 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.

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

✓ 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 Benutzerkennung über Bluetooth sollte nur bei Bedarf übertragen werden (Benutzerkennung 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 Benutzerkennung auf keinen Fall übertragen.

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!

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

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** („**B**ring **y**our **o**wn **D**evice“): **Bring dein eigenes Gerät mit** – und nutze es gleichzeitig für die Arbeit.

ANREGUNG FÜR DEN UNTERRICHT

Diskussionsfragen: Nutzen die Schüler 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, VERSCHLÜSSELUNG 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 FÜR DEN UNTERRICHT

Diskussionsfragen: Gibt es in den ausbildenden Unternehmen 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.

Jailbraking 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 Datenschutz-Aufsichtsbehörde zu melden. Dazu sind alle Unternehmen gesetzlich verpflichtet, die personenbezogene Daten verarbeiten.

ANREGUNG FÜR DEN UNTERRICHT

Diskussionsfragen: Haben die Ausbildungsbetriebe die private Nutzung von Geräten und Firmenmails geregelt? Gab 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

LERNEINHEIT 4: MOBILE UND PRIVATE ENDGERÄTE AM ARBEITSPLATZ

UNTERRICHTSVERLAUF

4 Schulstunden á 45 Minuten

1. SCHULSTUNDE

Thema	Inhalt und Methode	Arbeits-form	Material	Dauer
Vorbereitung	> Aufbau & Technik-Check			
Einstieg & Begrüßung	> Start mit SuS: Begrüßung und kurze Vorstellung	Plenum		5 Min
Diskussion: BYOD in Unternehmen und mögliche Risiken	> Diskussion im Plenum: Nutzen die SuS bzw. andere Mitarbeiter*innen ein privates Gerät bei der Arbeit? Welche Risiken müssen bei der Nutzung von mobilen Geräten, v.a. am Arbeitsplatz beachtet werden? > Brainstorming mit Hilfe einer Web-Anwendung. Beispiele: https://answergarden.ch https://www.mentimeter.com > Alternative: Sammlung an Tafel, Whiteboard, Flipchart o.ä.	Plenum	> Smartphones oder Computer mit Internetzugang, Brainstorming-App, Beamer oder Smartboard > Tafel, Whiteboard oder Flipchart	10 Min
PowerPoint Präsentation: Wiederholung Risiken von BYOD	> Präsentation der PowerPoint Folien 1 – 4 durch die Lehrkraft: - Einführung: BYOD - Sicherheitsrisiken mobiler Endgeräte > Ggfs. Diskussion im Plenum	Plenum	> Laptop oder PC > Beamer oder Smartboard > Speichermedium mit PowerPoint Präsentationsfolien LE 4	10 Min
Wissensvermittlung: Lehrfilm „Mobile Endgeräte im betrieblichen Kontext“	> Lehrfilm im Plenum schauen, an gekennzeichneter Stelle anhalten > Fragen im Plenum oder in Kleingruppen diskutieren > Zusammenfassung mit Hilfe einer Power-Point-Präsentation oder in Form eines Wikis Nützliche Wiki-Empfehlungen: https://lehrerfortbildung-bw.de/st_digital/medienwerkstatt/internet/cms/wiki/wikiengine.htm > Alternative: Zusammentragen der Regeln auf Poster, Tafel, Whiteboard bzw. Flipchart > Diskussion im Plenum > Film zu Ende schauen	Plenum Plenum oder Kleingruppen	> PC/Laptop > Beamer + Soundsystem oder Smartboard > Speichermedium mit Film oder Abspielen des Films über einen Internetzugang > PCs/Laptops für SuS > Tafel, Whiteboard, Poster oder Flipchart, Eddings	15 Min
Abschluss	> Ggfs. offene Fragen klären > Hausaufgabe (optional): SuS sollen einen Tipp für bessere mobile Sicherheit recherchieren, die den anderen in der nächsten Stunde vorgestellt wird – je nach Anzahl der Beteiligten auch als Gruppenarbeit. > Ausblick für die nächste Stunde > Ergebnissicherung: Die Lehrkraft fotografiert das Tafelbild > Wenn nicht Schulstunde 5 durchgeführt wird: Aushändigung des Transfermaterials (Poster, Checkliste, Arbeitsauftrag) sowie der ausgedruckten PowerPoint Folien als Handout		> Fotoapparat oder Smartphone > Ggfs. Transfermaterialien (Poster, Checkliste, Arbeitsauftrag etc.) & Handouts	5 Min

2. SCHULSTUNDE (ANMERKUNG: ZUSAMMENHÄNGEND MIT SCHULSTUNDE 3)

Thema	Inhalt und Methode	Arbeitsform	Material	Dauer
Vorbereitung	> Evtl. Aufbau einer „Bühne“ für das Planspiel			
Einstieg & Begrüßung	> Start mit SuS: Begrüßung und kurze Vorstellung	Plenum		5 Min
Rollenspiel: Sammlung von Daten durch Apps Teil I	> Rollenspiel Lerneinheit R4: „Neugierige Apps“: Briefingphase und Spielphase	Plenum	> Arbeitsbogen R4	40 Min

3. SCHULSTUNDE (ANMERKUNG: ZUSAMMENHÄNGEND MIT SCHULSTUNDE 2)

Thema	Inhalt und Methode	Arbeitsform	Material	Dauer
Rollenspiel: Sammlung von Daten durch Apps Teil II	> Rollenspiel Lerneinheit R4: „Neugierige Apps“: Auswertungsphase	Plenum	> Arbeitsbogen R4	20 Min
Sicherheitsregeln zur Nutzung von mobilen Geräten und BYOD	> Diskussion im Plenum: Welche Sicherheitsregeln sollten bei der Nutzung von mobilen Geräten, v.a. am Arbeitsplatz beachtet werden? (Wenn möglich Nutzung der in Schulstunde 1 gesammelten Punkte: Zu jedem Risiko eine Präventionsmaßnahme) > Zusammenfassung mit Hilfe einer PowerPoint Präsentation oder in Form eines Wikis Nützliche Wiki-Empfehlungen: https://lehrerfortbildung-bw.de/st_digital/medienwerkstatt/internet/cms/wiki/wikiengine.htm > Alternative: Zusammentragen der Regeln an der Tafel/auf einem Poster	Plenum	> Laptop/PC, Beamer oder Smartboard > Tafel, Whiteboard oder Flipchart, ggfs. Eddings	20 Min
Abschluss	> Ggfs. offene Fragen klären > Ausblick für die nächste Stunde > Ergebnissicherung: Die Lehrkraft fotografiert Poster/Tafelbild > Wenn nicht Schulstunde 5 durchgeführt wird: Aushändigung des Transfermaterials (Poster, Checkliste, Arbeitsauftrag) sowie der ausgedruckten PowerPoint Folien als Handout		> Fotoapparat oder Smartphone > Ggfs. Transfermaterialien (Poster, Checkliste, Arbeitsauftrag etc.) & Handouts (PowerPoint Folien LE4)	5 Min

4. SCHULSTUNDE

Thema	Inhalt und Methode	Arbeitsform	Material	Dauer
Vorbereitung	> Aufbau & Technik-Check			
Einstieg & Begrüßung	> Start mit SuS: Begrüßung und kurze Vorstellung	Plenum		5 Min
PowerPoint Präsentation: Wiederholung Sicherheitsregeln I	> Präsentation der PowerPoint Folien (Kap. 3) durch die Lehrkraft: Sicherheitsmaßnahmen > Ggfs. Diskussion im Plenum	Plenum	> Laptop oder PC > Beamer & Sound oder Smartboard > Speichermedium mit PowerPoint Präsentationsfolien LE 4	15 Min
Wissens-Check: Quiz	> Beantwortung des Quiz Q4 durch SuS auf Papier oder online auf der Bottom-Up Webseite unter www.dsin-berufsschulen.de > Alternativ: Bearbeiten der QR-Code-Rallye QR4 (Hinweis: diese Methode dauert etwa 10 - 15 Minuten länger, ggfs. die Diskussion kürzen) > Vergleich und Diskussion der Lösungen	Einzel- oder Gruppenarbeit Einzel- oder Gruppenarbeit Plenum	> Arbeitsbogen Q4 bzw. Smartphone o. Computer mit Internetzugang > ausgedruckte QR-Codes > Arbeitsbogen QR4 und Smartphones mit QR-Code-Scanner	20 Min
Abschluss	> Ggfs. offene Fragen klären > Ausblick für die nächste Stunde > Ergebnissicherung: Die Lehrkraft fotografiert die Poster > Wenn nicht Schulstunde 5 durchgeführt wird: Aushändigung des Transfermaterials (Poster, Checkliste, Arbeitsauftrag) sowie der ausgedruckten PowerPoint Folien als Handout		> Fotoapparat oder Smartphone > Ggfs. Transfermaterialien (Poster, Checkliste, Arbeitsauftrag etc.) & Handouts	5 Min

5. SCHULSTUNDE

Thema	Inhalt und Methode	Arbeitsform	Material	Dauer
Vorbereitung	> Aufbau > Evtl. Bildung von Gruppenarbeitstischen			
Einstieg & Begrüßung	> Start mit SuS: Begrüßung und kurze Vorstellung	Plenum		5 Min
Wissens-Check und Transferübung: Sicherheitsberatung zu mobilen Endgeräten	> Bildung von Kleingruppen > Lesen des Textes und Beantwortung der Fragen von AB 4 in der Kleingruppe. > Alternative: SuS lesen das Szenario und beantworten anschließend die Fragen in Einzelarbeit (Kann auch als LEK genutzt werden) > Diskussion der Ergebnisse im Plenum	Kleingruppen Ggfs. Einzelarbeit Plenum	> AB 4: Sicherheits-beratung zu mobilen Endgeräten im Unternehmen	25 Min
Abschluss	> Ggfs. offene Fragen klären > Aushändigung der ausgedruckten PowerPoint Folien als Handout > Aushändigung und kurze Erläuterung des Transfermaterials: Poster, Checkliste & Arbeitsauftrag		> Transfermaterialien (Poster, Checkliste, Arbeitsauftrag etc.) > Handouts (PowerPoint Folien LE 4)	10 Min

ROLLENSPIEL R4

ARBEITSANWEISUNG FÜR DIE LEHRKRAFT

Nach der Beschäftigung mit den theoretischen Inhalten soll nun eine konkrete, sicherheitskritische Situation in Form eines Planspiels bearbeitet werden. Die Schüler*innen schlüpfen in unterschiedliche Rollen und werden mit einem Szenario einer kritischen IT-Sicherheitsproblematik konfrontiert: der heimlichen Weitergabe von Daten durch mobile Apps. Auch wenn vielen bekannt ist, dass mittels mobiler Endgeräte Daten über die Nutzer erfasst und auch an Dritte weitergegeben werden, ist wenigen Menschen bewusst, was das für sie persönlich bedeutet. Durch das Rollenspiel soll den Schüler*innen deutlich werden, dass diese Datenlecks privat wie beruflich ein nicht zu unterschätzendes Risiko darstellen. Eine abstrakte Situation soll konkretisiert und erlebbar gemacht werden. Die Schüler*innen haben die Aufgabe, diese Situation gemeinsam zu erarbeiten und zu diskutieren. Dabei soll die eigene Erfahrung im Rollenspiel sie dazu ermutigen, die Problematik im Unternehmen anzusprechen und dort auf Lösungsansätze hinzuweisen.

Das Planspiel ist in drei Schritte unterteilt: Briefingphase – Spielphase – Auswertungsphase.

1. BRIEFINGPHASE

Das Ziel ist es, eine alltägliche Situation bewusst zu erleben und die möglichen Risiken und Probleme greifbar und wahrnehmbar zu machen. Die eine Hälfte der Schüler*innen soll im Rahmen des Planspiels die andere Hälfte in diese Situation versetzen und wird entsprechend gebrieft. Im Anschluss werden Empfehlungen zum zukünftigen Schutz vor dieser Sicherheitsproblematik erarbeitet.

Ausgangslage des Spiels: Das Szenario „Neugierige Apps“

In einem Ladengeschäft werden die Kund*innen beim Einkauf nach ihrer Telefonnummer, ihren Kontakten und/oder ihren letzten Aufenthaltsorten gefragt. Manche werden von den Verkäufer*innen bis auf die Straße verfolgt „um zu sehen, wo sie jetzt hingehen“. Das alles passiert „standardmäßig“ und „um den Service zu verbessern“. Die Kund*innen sind möglicherweise nicht immer einverstanden.

Die unterschiedlichen Rollen: Die Interaktion

Auf dieser Grundlage spielt jede*r Schüler*in eine*n Vertreter*in aus einer der Gruppen. In dieser zugewiesenen Rolle versuchen die Schüler*innen, ihre beschriebenen Standpunkte einzunehmen und zu vertreten.

> Die **„Verkäufer*innen“** versuchen möglichst viele Informationen und Daten durch geschicktes Befragen von den Kund*innen zu sammeln.

> Die **„Kund*innen“** sollten im Vorfeld nicht informiert werden und während der Briefingphase von der Gruppe der „Verkäufer“ getrennt sein (zum Beispiel auf dem Flur vor dem Klassenraum).

2. SPIELPHASE

Zunächst getrennt voneinander:

> Die **„Verkäufer*innen“** tragen gemeinsam Einfälle zusammen, wie sie Informationen von den Kund*innen abfragen können. Sie halten ihren Wissensstand fest: Welche Informationen fragen Apps und Webseiten eigentlich ab? Wie kann man das in ein simuliertes Verkaufsgespräch in einem Geschäft übersetzen?

> Die andere **Gruppe der „Kund*innen“** erstellt zunächst eine Übersicht darüber, welche Apps die Schüler*innen in ihrer Gruppe installiert haben und welche davon sie häufig nutzen (gegebenenfalls mit einer Darstellung in Rankingform). Das gleiche sollen sie für Internetseiten tun, die sie regelmäßig nutzen. Die Gruppe sollte zunächst nicht wissen, wofür diese Informationen erarbeitet werden. Sollte die Gruppendynamik dies erforderlich machen, kann ein*e Schüler*in „ernannt“ werden, um den Fortschritt der Gruppe zu beaufsichtigen, die für einen Teil der Unterrichtseinheit räumlich vom Rest der Klasse getrennt wird.

Rollenspiel:

Auf dieser Grundlage spielen die Schüler*innen verschiedene Einkaufssituationen so durch, dass jede*r einmal aktiv spielt. Dabei können die Fragen und Forderungen der „neugierigen Apps“ variiert werden. Die Gruppe der Kund*innen hat den Auftrag, so zu reagieren wie sie es im echten Leben tun würden.

Hinweise an die Spieler*innen:

> Freie und spontane Interaktion

> An die vorgegebenen Rollen und Vorgaben halten

> Realistisch bleiben

Hinweise an die Beobachter*innen:

> Keine Einmischung von außen

> Führen eines Beobachtungsbogens für die spätere Auswertung ist hilfreich

Requisiten:

> werden nicht benötigt. Um die Ware des Geschäfts zu simulieren, können Kleidungsstücke oder andere Gegenstände verwendet werden. Beobachter und Spielszene können räumlich getrennt werden, das Rollenspiel kann zum Beispiel in einer Ecke im Klassenraum gespielt werden.

Regeln:

Die Lehrkraft fungiert als Spielleitung und greift in die Handlung ein, sobald diese in eine Richtung abgleitet, die themen- und sicherheitsmäßig nicht relevant ist. Die Spielleitung sorgt für einen störungsfreien Ablauf und besitzt die Funktion bei Konflikten zwischen Personen einzugreifen. Während der gesamten Rollenspielphase sorgt die Spielleitung dafür, dass die Rollen von den Schüler*innen ernst genommen werden.

3. AUSWERTUNGSPHASE

Im Anschluss an das Planspiel erfolgt eine gemeinsame Spielanalyse mit einer Bewertung des Szenarios und einer Kritik an den Lösungsschritten.

Bei der Auswertung werden in der Regel vier Phasen unterschieden:

1. Intuitive Spielanalyse (Was ist passiert? Was haben die Spieler*innen empfunden?)

2. Spielreflexion und Distanzierung (Wie lässt sich der Spielverlauf erklären? Wie bewerten die Gruppen das Spielergebnis? Was hat das Ergebnis beeinflusst?)

3. Transfer (Welche Aspekte des Szenarios und des Spielverlaufs waren realistisch, welche nicht? Welche Relevanz hat das Ergebnis des Planspiels für unseren Blick auf die Realität?)

4. Spielkritik (Was haben wir gelernt? Was nicht? Was nehme ich persönlich mit? Wie könnte man das Spiel verbessern?)

Leitfragen, die es außerdem zu klären gilt:

1. Warum finden wir es im „echten“ Leben problematisch, von unbekannten Personen ausgefragt und verfolgt zu werden, lassen es aber mittels unserer Handys, Tablets und Computern über uns ergehen?

2. Wo sind die Unterschiede? Sollte es Unterschiede in unserer Reaktion geben?

3. Was ändert sich, wenn unter den letzten Aufenthaltsorten geschäftliche Treffen waren, und unter den letzten gewählten Nummern vertrauliche Kundengespräche?

4. Was sind die Gefahren? Wie können wir uns schützen?

Dabei kann sowohl auf das Theoriemodul zurückgegriffen werden, als auch auf die Ergebnisse der Gruppe, die festgehalten hatte, welche Apps häufig genutzt werden. Die Schülerinnen und Schüler können diskutieren, welche Zugriffsrechte diese Apps verlangen und wie sie dies nunmehr bewerten. Sie können Beschlüsse für das eigene Verhalten fassen und eventuell stichpunktartig festhalten, um diese Beschlüsse als Tipps in die Unternehmen zu tragen. Bei Bedarf kann die Lehrkraft Input liefern und bei der Verortung des Rollenspiels in der Lebenswelt der Schülerinnen und Schüler behilflich sein.

Beispiele für Lösungselemente: Apps sollten nur die Zugriffsrechte zugewiesen kommen, die für ihr Funktionieren nötig sind (eine Taschenlampen-App braucht zum Beispiel keinen Zugriff auf das Adressbuch). Bei vielen Smartphones lassen sich die Zugriffsmöglichkeiten für Apps einstellen und die Zugriffsrechte schon vor dem Installieren prüfen. Die GPS-Lokalisierungsfunktion sollte nur bei Bedarf aktiviert werden, und ansonsten ausgestellt bleiben. Gleiches gilt für WLAN und Bluetooth-Verbindungen, da auch hierüber Bewegungsprofile erstellt werden können.

ARBEITSBOGEN AB4: SICHERHEITSBERATUNG ZU MOBILEN ENDGERÄTEN IM UNTERNEHMEN

LÖSUNG FÜR DIE LEHRKRAFT

Beschreibung

Bei dem dargestellten Szenario sollen die Schüler*innen mögliche Risiken hinsichtlich mobiler und möglicherweise privater Endgeräte im Unternehmen erkennen und hierzu die Fragen entsprechend beantworten. Dies kann in Einzel- oder Gruppenarbeit geschehen.

Diese Aufgabe kann auch als Lernerfolgskontrolle genutzt werden.

Lösung:

1. Der Auszubildende sollte versuchen, das Gerät zu lokalisieren und die Daten aus der Ferne zu löschen. Auch wenn das nicht möglich ist, sollte er seine SIM-Karte sperren lassen. Weil personenbezogene Daten von Kunden auf dem Gerät gespeichert sind, muss das Unternehmen offiziell informiert werden, damit es den Verlust bei der Datenschutzbehörde melden kann. Wichtig für die Zukunft sind: PIN und Bildschirmsperre, Dateien auf dem Gerät verschlüsseln bzw. Backups anlegen, keine sensiblen Daten auf Mobilgeräten speichern und Einstellungen zum Orten bzw. Fernlöschen anpassen.
2. Herr Zahl sollte seine geschäftlichen Mails nicht jeden Monat löschen, da für Unterlagen wie Rechnungen eine gesetzliche Aufbewahrungspflicht besteht. Auch er sollte die unter 1 genannten Hinweise beherzigen und vorsichtig mit der Nutzung von öffentlichen WLAN-Hotspots sein sowie eine Verschlüsselung für E-Mails nutzen.
3. Herr Cosimo sollte den Zugriff der Taschenlampen-App auf die gespeicherten Kontakte unterbinden. Wenn die Einstellungen seines Smartphones das nicht erlauben, sollte Herr Kaufmann die App entfernen.
4. Frau López sollte keine ungeschützten WLAN-Netzwerke verwenden. Hotspots in Flughäfen sind oft ungesichert. Das muss nicht immer so sein, es ist aber zunächst Vorsicht geboten.
5. Die private Kommunikation der Mitarbeiter*innen ist durch das Fernmeldegeheimnis geschützt. Auch wenn Unternehmenssoftware auf privaten Geräten installiert ist, darf das Unternehmen nicht auf private Inhalte zugreifen.
6. Dies ist eine freie Schreibaufgabe. Korrekte Vorschläge können zum Beispiel sein:
   - > Die IT-Verantwortlichen sollten darüber informiert werden, wenn private Geräte für die Arbeit genutzt werden (Verbindung mit Unternehmens-Netzwerk/Speicherung von Geschäftsdaten).
   - > Alle Mitarbeiter*innen sollten darüber aufgeklärt werden, welche Sicherheitsrisiken durch BYOD entstehen.
   - > Die IT-Verantwortlichen könnten eine Liste mit sicheren Apps erstellen.
   - > Es könnte eine spezielle MDM-Software eingeführt werden, um die Sicherheit der Unternehmensdaten auf den privaten Geräten professionell zu gewährleisten.
   - > Weitere richtige Antworten sind denkbar.

ARBEITSBOGEN AB4: SICHERHEITSBERATUNG ZU MOBILEN ENDGERÄTEN IM UNTERNEHMEN

ARBEITSANWEISUNG FÜR DIE SCHÜLER*INNEN

Arbeitsauftrag

1. Lesen Sie das Szenario aufmerksam durch.
2. Beantworten Sie dann die untenstehenden Leitfragen.

Leitfragen

a) Was raten Sie dem Auszubildenden?

b) Welche rechtlichen Anforderungen sollte der Buchhalter Herr Zahl beachten?

c) Welchen Tipp geben Sie Herrn Cosimo?

d) Wovon raten Sie der reisenden Mitarbeiterin Frau López in Zukunft ab?

e) Wie beruhigen Sie die Betriebsrätin?

f) Entwickeln Sie mindestens zwei Vorschläge, die für eine interne BYOD-Richtlinie ratsam sind. Diese Aufgabe gilt für alle Unternehmen und ist nicht auf das Unternehmen Mustermann beschränkt.

Das Szenario

Sie sind als Expertin bzw. Experte für eine Sicherheitsberatung bei dem Logistikunternehmen Venti eingeladen und sehen sich in dem Betrieb um. Als erstes fällt Ihnen ein Auszubildender auf, der voller Wut feststellt, dass das Tablet gestohlen wurde, auf dem er gerade erst am Vortag die Adressen der Kunden gespeichert hatte, die heute besucht werden sollten!

Nachdem Sie mit ihm über mögliche Lösungen und zukünftige Sicherheitsvorkehrungen gesprochen haben, treffen Sie Herrn Zahl aus der Buchführung. Herr Zahl hat sich vor kurzem sein erstes Smartphone angeschafft und legt großen Wert darauf, alles schön aufgeräumt zu halten. Er löscht seine Mails jeden Monat, damit das Postfach übersichtlich bleibt. Er lässt sich gerade von einer Kollegin erklären, wie er auch sein berufliches Mailkonto per App öffnen kann, damit er unterwegs Kundenmails beantworten kann. Denn Herr Zahl bekommt täglich verschiedene Rechnungen für das Unternehmen und hat eine lange Bahnfahrt zur Arbeit, die er zum Lesen der Nachrichten nutzen möchte. Sie weisen Herrn Zahl auf eine rechtliche Verpflichtung im Umgang mit seinen geschäftlichen Mails hin und verlassen die Buchhaltungsabteilung.

Im Vertrieb freut sich gerade Herr Cosimo über seine neue Taschenlampen-App. Als Sie mit ihm die Zugriffsberechtigungen der App ansehen, fällt Ihnen auf, dass die App Zugriff auf die gespeicherten Kontakte hat. Herr Cosimo hat viele Telefonnummern von Kunden auf seinem Smartphone gespeichert. Sie geben ihm einen Tipp und gehen weiter zur nächsten Mitarbeiterin.

Die Mitarbeiterin Frau López kommt gerade von einer Dienstreise. Sie hat im Ausland eine neue Geschäftsidee getestet, die noch streng geheim ist. Sie beschwert sich gerade, dass der Hotspot am Flughafen mal wieder völlig überlastet war und dass sie eine sehr schlechte Verbindungsgeschwindigkeit hatte. Sie sprechen eine Warnung aus und begeben sich zu Ihrem letzten Termin beim Unternehmen.

Die Vorsitzende des Betriebsrats Frau Mertens ist wegen Ihrer Anwesenheit besorgt. Sie hat von einer Kontrollsoftware gehört, mit der die privaten Geräte von Mitarbeitern vom Arbeitgeber überwacht werden können und fürchtet nun um die Privatsphäre der Mitarbeiter.

Nachdem Sie ihr ihre Sorgen genommen haben, gehen Sie zufrieden in Ihr Büro und schreiben ein Beratungsprotokoll für die Geschäftsführung des Unternehmens.

ARBEITSBOGEN: QUIZ Q4

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

QR-CODE-RALLYE QR4

ARBEITSANWEISUNG FÜR DIE LEHRKRAFT

Beschreibung

1. Die folgenden QR-Codes ausdrucken, ausschneiden und einzeln an verschiedenen Stellen im Klassenraum anbringen.
2. Die Schüler*innen erhalten den Fragebogen, den sie mit Hilfe der QR-Codes beantworten können. Hinter jedem Code verbirgt sich eine richtige Antwort, die auf dem Display angezeigt wird, wenn der Code mit einer QR-Code-Scanner-App eingescannt wird (diese muss ggfs. installiert werden, bitte beachten Sie die Hinweise dazu aus Lerneinheit 4: insb. Zugriffsrechte prüfen!).
3. Die Schüler*innen schreiben die richtige Antwort unter die passende Frage auf ihrem Arbeitsblatt. Den Buchstaben des QR-Codes setzen sie in das Kästchen der entsprechenden Frage. So erhalten sie am Ende ein Lösungswort.

G

N

H

H


I


I


S


P

QR-CODE-RALLYE QR4

LÖSUNG FÜR DIE LEHRKRAFT

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

   Um anhand der Nutzerdaten zum Beispiel gezielte Werbung einzuspielen.

P

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

   Jeder, der das Gerät in die Hände bekommt, kann auf die gespeicherten Daten zugreifen.

H

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

   Man sollte sie vom Netzbetreiber sperren lassen.

I

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

   Aus Datenschutz-Gründen: die WLAN-Funktion kann auch dafür verwendet werden, Bewegungsprofile zu erstellen.

S

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

   Man geht sicher, dass die Sicherungskopie lesbar ist, indem man einige Daten kopiert und prüft.

H

6. **Was ist bei einer internen BYOD-Richtlinie für das Unternehmen besonders wichtig?**

   Dass sich alle Mitarbeiter*innen an die Regeln halten. Schon ein einzelnes unsicheres Gerät ist ein Risiko für das Unternehmen.

I

7. **Auf einem privaten mobilen Endgerät befinden sich Kundendaten des Unternehmens. Wer darf darauf zugreifen?**

   Nur der/die Mitarbeiter*in, dem das Gerät gehört und eventuell andere Mitarbeiter*innen des Unternehmens.

N

8. **Kann ich als Mitarbeiter*in ein mobiles Endgerät bei der Arbeit genauso nutzen wie privat?**

   Nein, manche Apps sind privat kostenlos, kosten für Unternehmen aber Geld. Das muss für jede App überprüft werden.

G

QR-CODE-RALLYE QR4

ARBEITSBOGEN FÜR DIE SCHÜLER*INNEN

Arbeitsauftrag

1. Installieren Sie auf Ihrem Smartphone einen QR-Code-Scanner. Wichtig: prüfen Sie zuvor die Zugriffrechte und Vorsicht bei Drittanbieter-Stores!
2. Hinter jedem der im Raum verteilten Codes verbirgt sich eine richtige Antwort, die auf dem Display angezeigt wird, wenn der Code mit einer QR-Code-Scanner-App eingescannt wird. Finden Sie für jede der folgenden Frage die passende Antwort und notieren Sie diese.
3. Den Buchstaben des QR-Codes setzen Sie in das Kästchen der entsprechenden Frage. In abfallender Reihenfolge ergeben alle Buchstaben das richtige Lösungswort.

1. Warum sammeln viele Apps heimlich Informationen über Nutzer?

_____

_____

_____

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

_____

_____

_____

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

_____

_____

_____

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

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

6. **Was ist bei einer internen BYOD-Richtlinie für das Unternehmen besonders wichtig?**

7. **Auf einem privaten mobilen Endgerät befinden sich Kundendaten des Unternehmens. Wer darf darauf zugreifen?**

8. **Kann ich als Mitarbeiter*in ein mobiles Endgerät bei der Arbeit genauso nutzen wie privat?**

ARBEITSAUFTRAG LE4: MOBILE UND PRIVATE ENDGERÄTE AM ARBEITSPLATZ

ARBEITSANWEISUNG FÜR DIE LEHRKRAFT

Ziel

Die Arbeitsaufträge und die bereitgestellten Transfermaterialien unterstützen die Schüler*innen, das erworbene Wissen zum Thema IT-Sicherheit in die Ausbildungsbetriebe zu tragen. Sie fördern damit die praktische Anwendung des im Unterricht gelernten Sicherheitswissens.

Mit Hilfe der folgenden Schritt-für-Schritt-Anleitung können die Schüler*innen die vermittelten Inhalte der Lerneinheit 4 „Mobile und private Endgeräte am Arbeitsplatz“ dialogorientiert und interaktiv mit Vorgesetzten und Kolleg*innen thematisieren.

Beschreibung

Teilen Sie den Arbeitsauftrag zur LE4 *Mobile und private Endgeräte am Arbeitsplatz* sowie das Anschreiben für den Ausbildungsbetrieb an die Schüler*innen aus. Zur Erfüllung des Arbeitsauftrags benötigen die Schüler*innen zudem folgende Transfermaterialien:

- Quiz aus LE4 (Entweder in Printform austeilen oder per digitalem Zugriff über die Bottom-Up Webseite unter http://t1p.de/vkh3)
- Checkliste zu LE4
- Poster 2 – IT-Sicherheit betrifft jeden! 5 Tipps für mehr mobile Sicherheit

Hinweis

Die Schüler*innen sollten selbst entscheiden, ob sie die einzelnen Arbeitsaufträge gestaffelt nach jeder Lerneinheit im Betrieb durchführen, oder ob sie am Ende der letzten Unterrichtseinheit einen größeren Arbeitsauftrag mit allen Lerneinheiten durchführen.

Die Festlegung eines Durchführungstermins für die Arbeitsaufträge wird empfohlen. Die Ausgabe der Teilnahmebescheinigung ist im besten Fall an die erfolgreiche Ausführung des Arbeitsauftrags gekoppelt.

ARBEITSAUFTRAG LE4:
MOBILE UND PRIVATE ENDGERÄTE AM ARBEITSPLATZ

ARBEITSBOGEN FÜR DIE SCHÜLER*INNEN

Zuvor

> Geben Sie Ihrer bzw. Ihrem **Vorgesetzten** das beigefügte Anschreiben.

> Bitten Sie, diesen Arbeitsauftrag mit dem Vorgesetzten durchzuführen. Alternativ ist auch die Umsetzung mit Kollegen möglich.

> Das gesamte Vorhaben dauert ca. 20 – 30 Minuten.

Durchführung

1. Erklären Sie Ihrem Vorgesetzten/Ihren Kollegen kurz Ihr Vorhaben.
2. Führen Sie das **Online-Quiz** 4 „Mobile und private Endgeräte am Arbeitsplatz“ durch (Das Quiz ist auf der Bottom-Up Webseite unter http://t1p.de/vkh3 verfügbar. Alternativ erhalten Sie den Arbeitsbogen in Printform von Ihrer Lehrkraft).
3. Diskutieren Sie mit den Teilnehmenden über die richtigen Lösungen.
4. Stellen Sie die **Checkliste** 4 „Sicherer Einsatz mobiler Endgeräte und BYOD“ vor und geben Sie jeweils ein Exemplar an die Teilnehmenden weiter. Gehen Sie danach gemeinsam die Checkliste durch und überprüfen Sie die aufgelisteten Punkte. (Die Checkliste erhalten Sie von Ihrer Lehrkraft)
5. Hängen Sie das **Poster 2** – IT-Sicherheit betrifft jeden! 5 Tipps für mehr mobile Sicherheit – auf und besprechen Sie gemeinsam die vorgestellten Verhaltensempfehlungen (Das Poster erhalten Sie von Ihrer Lehrkraft).
6. Installieren Sie sich gemeinsam die **SiBa-App** von DsiN und schauen Sie gemeinsam über die neusten Meldungen zu Bedrohungen durch Schadsoftware und Betrügereien (Über die Seite https://www.sicher-im-netz.de/ratgeber-tools-ratgeber-tools-fuer-alle/siba-aktuelle-meldungen gelangen sie zum Download Ihres jeweiligen App-Stores).

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

Anschreiben *IT-Sicherheit im Ausbildungsbetrieb*

Berlin, August 2017

Sehr geehrte Damen und Herren,

Ihr Auszubildender / Ihre Auszubildende nimmt an einer Schulung zu IT-Sicherheit und Datenschutz teil. Für den erfolgreichen Abschluss der Schulung ist die Ausführung eines Arbeitsauftrags nötig, mit dem das neu Erlernte in der Praxis angewandt wird. Wir bitten Sie daher kurz um Ihre Unterstützung und Mithilfe.

Der Schutz der IT und Daten spielt eine immer wichtigere Rolle für Unternehmen und Betriebe. Schon kleine Beeinträchtigungen in der Verfügbarkeit von Systemen, Endgeräten oder Daten können heutzutage unangenehme Folgen mit sich bringen. Der Faktor Mitarbeiter spielt hierbei eine tragende Rolle: Unsachgemäße Handhabung, Nachlässigkeit und sehr häufig ein fehlendes Sicherheitsbewusstsein sind hier Risikoquellen.

Nur regelmäßige Mitarbeiterschulungen können Abhilfe schaffen. Hier setzt das Lehrangebot *Bottom-Up* jetzt bereits in der Berufsschule an: Auszubildende werden anhand praxisnaher Lehrmaterialien auf die Herausforderungen der Digitalisierung im Arbeitsalltag vorbereitet.

Die Durchführung des Arbeitsauftrags nimmt zehn bis fünfzehn Minuten in Anspruch. Wir würden uns freuen, wenn Sie Ihren Auszubildenden / Ihre Auszubildende unterstützen – auch für mehr IT-Sicherheit in Ihrem Ausbildungsbetrieb! Mehr Informationen zum Projekt finden Sie unter www.dsin-berufsschulen.de.

Mit freundlichen Grüßen

Sascha Wilms
Projektleiter

Über Deutschland sicher im Netz e.V.
Produktneutral und herstellerübergreifend leistet DsiN als zentraler Ansprechpartner für Verbraucher*innen und mittelständische Unternehmen konkrete Hilfestellungen für mehr Sicherheitsbewusstsein im Netz.
Informieren Sie sich über alle Angebote von DsiN unter: www.sicher-im-netz.de

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 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**

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

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:
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

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.