HANDREICHUNG

FÜR WORKSHOPLEITER*INNEN

Berufsschüler BOTTOM-UP! für IT-Sicherheit

ww.dsin-berufsschulen.de

HANDREICHUNG FÜR WORKSHOPLEITER*INNEN

Diese Handreichung sowie die entsprechenden Materialien sollen dazu befähigen, einen **Workshop zum Thema IT-Sicherheit und Schutz von Daten** durchzuführen. Diese Schulung kann dabei als **Fortbildung für Lehrkräfte** genutzt werden, um sie generell zum Thema zu sensibilisieren, aber auch um sie zur Umsetzung des Lehrangebots *Bottom-Up* zu befähigen. Außerdem kann der Workshop in kleinen und mittleren Unternehmen (KMU) als **Mitarbeiterschulung** durchgeführt werden, um die wichtigsten Kenntnisse zum Thema IT-Sicherheit zu vermitteln.

Der Workshopleiter kann dabei eine Person aus dem Kollegium sein, oder auch eine externe Fachkraft. Auch können teilnehmende Berufsschüler – soweit sie sich dazu befähigt fühlen - die Handreichung verwenden, um einen ersten Workshop für Kollegen in ihrem Ausbildungsbetrieb zum Thema durchzuführen.

Die Handreichung stellt zunächst den Projektträger **DsiN e.V.** und das Lehrangebot ***Bottom-Up: Berufsschüler für IT Sicherheit*** vor. Im Anschluss werden die wichtigsten Aspekte **der sieben Lerneinheiten** zusammengefasst. Zum Abschluss werden **hilfreiche Tipps zu Unterrichtsvorbereitung**, Wissensvermittlung, Wissensabfrage und Visualisierung der Schulung vorgestellt.

DIE THEMEN:

*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. DAS ANGEBOT „BOTTOM-UP“

Der Verein **Deutschland sicher im Netz e. V**. (DsiN) entstand 2006 als Ergebnis des ersten IT-Gipfels der Bundesregierung. Er steht seit Juni 2007 unter der Schirmherrschaft des Bundesministeriums des Innern und setzt sich derzeit aus 24 Unternehmen, Verbänden sowie gemeinnützigen Organisationen zusammen. Sein Hauptanliegen besteht darin, bei Verbrauchern und in Unternehmen ein **Bewusstsein für einen sicheren Umgang mit Internet und IT** zu fördern sowie einen praktischen und messbaren Beitrag für mehr IT-Sicherheit zu leisten.

In diesem Rahmen hat DsiN unter anderem das Projekt ***Bottom-Up: Berufsschüler für IT-Sicherheit*** entwickelt. Ziel dabei ist es, speziell die künftigen Mitarbeiter kleiner und mittlerer Unternehmen über die steigenden Anforderungen an den Schutz vorhandener Daten und die Sicherheit der eigenen IT-Infrastruktur ausreichend zu informieren und zu sensibilisieren, sowie Lehrkräfte in dieser Thematik mit Hilfe von Schulungen fortzubilden. Das Lehrangebot umfasst aktuell **sieben Lerneinheiten**, die in ihrer Gesamtheit alle relevanten Themen mit dem Fokus auf die besonderen Gegebenheiten in kleinen in mittleren Unternehmen abdecken. Ausführliche Informationen dazu bietet das eigens dafür ins Leben gerufene Internetportal www.dsin-berufsschulen.de**.**

2. BEDEUTUNG DER IT-SICHERHEIT IN KMU

Selbst im kleinsten Handwerksbetrieb dürften mittlerweile in irgendeiner Form elektronische Kunden- und Lieferantendaten gespeichert und verarbeitet werden, weshalb das Thema IT-Sicherheit im Prinzip für alle Unternehmen relevant ist. Allerdings gibt hier in vielen Unternehmen nach wie vor in unterschiedlichen Facetten **Verbesserungs- und Optimierungsbedarf** – dies hat unter anderem auch wieder der ***DsiN-Sicherheitsmonitor Mittelstand 2016*** gezeigt. Danach können sich die unternehmensinternen IT-Schutzvorkehrungen viel zu oft nicht an zertifizierten Anforderungen wie dem vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegebenen IT-Grundschutz messen lassen. Dabei ist ein Schutzniveau auf dem aktuellen Stand der Technik sowie unter Berücksichtigung aktuell gültiger rechtlicher bzw. organisatorischer Vorgaben nicht nur aus Gründen eines ungestörten Betriebsablaufs wichtig, sondern auch wegen der möglichen finanziellen Konsequenzen im Fall von Schadensersatzansprüchen.

ANREGUNG FÜR DIE SCHULUNG

Das Thema IT-Sicherheit muss als ein Selbstverständnis aufseiten von Berufsschullehrkräften und Mitarbeitern von KMU wahrgenommen werden. Verdeutlichen Sie die Bedeutung und knüpfen Sie an den privaten Umgang mit IT an – so entsteht außerdem ein persönlicher Mehrwert für die Teilnehmenden, indem Sie ihr neues Sicherheitswissen auch im eigenen digitalen Alltag nutzen können.

3. GRUNDLEGENDE ASPEKTE DER IT-SICHERHEIT IN KMU: ZUSAMMENFASSUNG DER WICHTIGSTEN INHALTE AUS DEN LERNEINHEITEN 1-7

3.1. GRUNDEINTELLUNGEN FÜR EINEN SICHEREN ARBEITSPLATZ (LE 1)

Die Schlagworte „**Schadprogramme**“ oder „Malware“ (Abkürzung von engl. „malicious Software“ = Schadsoftware) sind heutzutage ein Oberbegriff für solche Programme, die sich in andere Programme oder Dateien einschleusen, sich selber verbreiten und Schadfunktionen ausführen. So kann Schadsoftware etwa Veränderungen an Hardware, dem Betriebssystem sowie der auf einem Rechner installierten Anwendungssoftware vornehmen und dadurch die Computersicherheit erheblich gefährden. Beispiele für Schadprogramme sind **Trojaner, Viren, und Würmer**. Ebenso vielseitig wie die Arten sind die Verbreitungswege der Schadprogramme: Dafür kommen Wechseldatenträger, Netzwerke und infizierte Webseiten ebenso in Frage wie E-Mails mit infizierten Dateianhängen, Downloads oder Instant Messenger.

VERTIEFUNG

Ergänzende Informationen über Schadprogramme und Verbreitungswege finden Sie im Skript der Lerneinheit 1 auf den Seiten 3-6.

VERBREITUNGSWEGE VON SCHADSOFTWARE

ANREGUNG FÜR DIE SCHULUNG

Erklären Sie hier die Grafik genauer. Einigen Teilnehmern sind durchaus nicht alle gezeigten Verbreitungswege ein Begriff.

Gebräuchliche technische Maßnahmen zur Abwehr von Schadsoftware stellen **Antiviren-Programme** und Firewalls dar. Erstere dienen dazu, bekannte Computerviren aufzuspüren, zu blockieren und zu beseitigen. Hierbei steht Nutzern eine Vielzahl von Programmen unterschiedlicher Anbieter zur Verfügung.

Eine **Firewall** schützt dagegen den PC oder das Netzwerk vor Zugriffen von außen, indem der durch die Firewall laufende Datenverkehr überwacht wird und Netzwerkzugriffe beschränkt bzw. unterbunden werden. Um einen bestmöglichen Schutz zu erzielen, sollte man Firewalls und Antiviren-Programme parallel nutzen.

VERTIEFUNG

Ergänzende Informationen über sinnvolle Sicherheitsvorkehrungen bei Anwendersoftware finden Sie im Leseskript der Lerneinheit 1 auf den Seiten 10 bis 12.

Nicht zuletzt kommt es darauf an, stets nur **Passwörter** mit ausreichend hoher Sicherheit zu verwenden. Passwörter bieten nach derzeitigem Stand der Technik dann eine hohe Sicherheit, wenn sie aus mindestens zwölf Zeichen bestehen sowie Groß- und Kleinbuchstaben mit Ziffern und Sonderzeichen kombinieren. Da sich mit immer längerer Nutzungsdauer eines bestimmten Passworts – unabhängig von seiner Komplexität – die Gefahr erhöht, dass es gehackt und missbraucht wird, sollten Passwörter regelmäßig geändert werden.

VERTIEFUNG

Ergänzende Informationen über die Sicherheit von Passwörtern finden Sie im Leseskript der Lerneinheit 1 auf den Seiten 13 und 14.

3.2 SICHERE DIGITALE KOMMUNIKATION IM BERUFLICHEN KONTEXT (LE 2)

Um die IT-Sicherheit in einem Unternehmen zu gewährleisten, müssen alle Mitarbeiter geschult und entsprechend informiert sein.

Um Kunden- und Mitarbeiterdaten, aber auch Firmenwissen vor Manipulation oder vor dem Ausspähen etwa durch konkurrierende Unternehmen zu schützen, ist Sicherheit in der Kommunikation von entscheidender Bedeutung. Um dies zu erreichen, müssen alle betreffenden Mitarbeiter entsprechend informiert und instruiert werden. Dabei ist zu beachten, dass neben dem klassischen Kommunikationskanal „**E-Mail**“ zunehmend **alternative Kommunikationsmöglichkeiten** wie etwa Web-Blogs genutzt werden.

E-Mail-Nachrichten sind nach wie vor das mit Abstand größte Einfallstor für Schadsoftware oder sonstige Angriffe wie etwa Phishing-Attacken. Die größte Gefahr lauert dabei jeweils in den **Dateianhängen**, denn darin können sich die unterschiedlichsten Schadprogramme wie Spyware (Spionage-Software) oder Ransomware (Verschlüsselungs-Software) verbergen. Aus diesem Grund ist die Regel „öffne niemals Dateianhänge von E-Mails unbekannter Absender“ eisern einzuhalten.

ANREGUNG FÜR DIE SCHULUNG

Was sind Phishing-Attacken? Geben Sie den Teilnehmern ein aktuelles Beispiel.

Achtung! Schadprogramme können Dateiendungen vortäuschen informiert sein.

Aber auch E-Mails von bekannten Absendern sollte man kritisch prüfen, weil sich die Absenderkennung relativ leicht fälschen lässt. Aus diesem Grund sollte man bei Dateianhängen von E-Mails immer folgende **Hinweise** beachten:

> **Text- und Office-Dateien**: Reine Textdateien mit der Endung .TXT sind in der Regel als sicher zu betrachten. Allerdings können Schadprogramme (wie bei allen anderen Dateien auch) eine .TXT-Endung vortäuschen – die Datei endet dann in Wirklichkeit aber zum Beispiel auf .TXT.EXE. Dateien mit der Endung .PDF können in der Regel nur durch bestehende Sicherheitslücken im Adobe Reader gefährlich werden. .DOC(X), .XLS(X) und .PPT(X) können so genannte Makroviren enthalten. Hier bietet sich an, Makros zu deaktivieren oder sich die Dateien mit Programmen anzeigen zu lassen, die keine Makros unterstützen.

> **Komprimierte Dateien**: Dateien mit den Endungen .ZIP und .RAR werden nicht selten zum Übertragen von Schadsoftware genutzt.

> **Bilddateien**: .JPG und .GIF können potentiell mit Schadsoftware beladen sein.

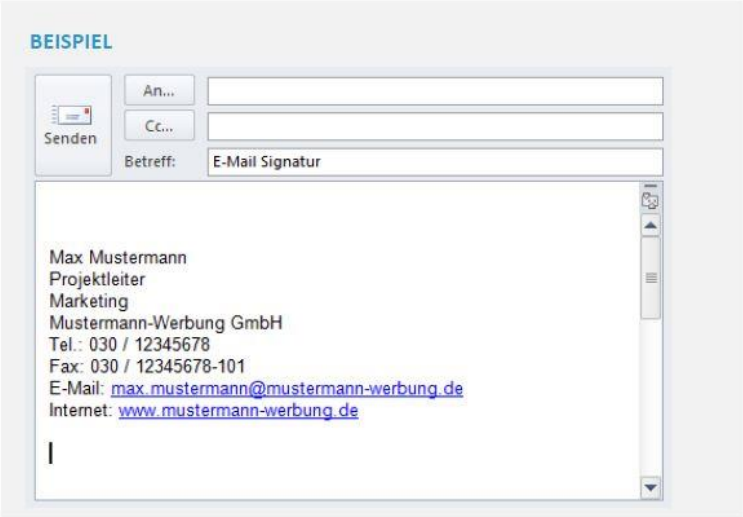
Zur Sicherheit sollte man sich in jedem Fall die Dateiendung vor dem Öffnen der Datei im E-Mail-Programm oder im Dateisystem komplett anzeigen lassen. Des Weiteren sollten Anhänge nur dann geöffnet werden, wenn der Absender sorgfältig geprüft wurde: Stammt die E-Mail wirklich von dem genannten Absender? Und ist die Übersendung des Anhangs plausibel? Im Übrigen können auch E-Mails ohne Dateianhang gefährlich sein, wenn sie einen Link zu einer infizierten Webseite enthalten.

Ende-zu-Ende-Verschlüsselung: Die Nachricht ist während der gesamten Übertragung verschlüsselt und kann nur vom Empfänger wieder entschlüsselt werden.

Um das Risiko zu minimieren, dass E-Mails während des Transports verändert (gefälscht) werden, sollte in allen E-Mail-Accounts sowohl beim Posteingangsserver als auch beim Postausgangsserver die **Transportverschlüsselung** (SSL/TLS) aktiviert sein. Und um zu verhindern, dass der Inhalt einer E-Mail von Dritten mitgelesen wird, empfiehlt sich die Nutzung der so genannten Ende-zu-Ende-Verschlüsselung. Dabei wird eine E-Mail vom Sender auf seinem Rechner verschlüsselt und kann vom Empfänger nur mit Hilfe eines Schlüssels wieder entschlüsselt werden. Daher sollte man insbesondere sensible Informationen nur auf diesem Wege versenden.

Zusätzliche Sicherheit bei der E-Mail-Kommunikation kann die Verwendung **elektronischer Signaturen** bieten. Dabei sind die fortgeschrittene elektronische Signatur sowie die qualifizierte elektronische Signatur zu unterscheiden. Beide Verfahren stellen die Authentizität und Unverfälschtheit der durch sie signierten Daten anhand asymmetrischer Verschlüsselungsverfahren sicher. Während es aber die fortgeschrittene elektronische Signatur im Prinzip nur erlaubt, die Authentizität des Absenders zu überprüfen, kann eine qualifizierte elektronische Signatur durch zusätzliche Sicherheitsmerkmale sogar die in Deutschland per Gesetz oder Verordnung geforderte notwendige Schriftform, die für einige Verträge und notarielle Beglaubigungen gilt, ersetzen.

Die Verwendung elektronischer Signaturen ist in der Geschäftskommunikation gesetzlich vorgeschrieben.



Bei der E-Mail-Kommunikation lauern im Übrigen nicht nur Gefahren durch Phishing und Schadsoftware, sondern auch **rechtliche Fallstricke**. So dürfen aus datenschutzrechtlichen Gründen personenbezogene Daten in Deutschland grundsätzlich nur mit Einwilligung des Betroffenen übertragen werden. Dies ist unter anderem im Zusammenhang mit dem Versand von Newslettern relevant, weil man zum Beispiel die E-Mail-Adresse einer Person nicht ohne deren vorherige Einwilligung für andere Personen sichtbar machen – also etwa in das cc-Feld setzen – darf. Außerdem ist gesetzlich vorgeschrieben, dass am Ende einer geschäftlichen E-Mail eine Signatur zu stehen hat – analog zu einem Geschäftsbrief. Abhängig von der Rechtsform der Firma müssen darin spezielle Angaben gemacht werden, dazu gehören unter anderem die Namen der Geschäftsführer und Aufsichtsratsvorsitzenden. Das gilt für alle E-Mails – egal, ob an Geschäftspartner oder Kunden.

Auch für die **Kommunikation über Webseiten wie Blogs oder Social-Media-Plattformen** sind mittlerweile hohe Sicherheitsanforderungen zu beachten. Gemäß Telemediengesetz müssen geschäftlich betriebene Internetseiten gegen Verletzungen des Schutzes von personenbezogenen Daten abgesichert sein. Das heißt konkret, dass beispielsweise Kontaktformulare die eingegebenen Daten nur auf verschlüsseltem Wege – erkennbar an der Internetadresse „https://...“ übertragen dürfen.

ANREGUNG FÜR DIE SCHULUNG

Zeigen Sie eine verschlüsselte Internetadresse im Webbrowser! Womöglich ist dies nicht allen Teilnehmern ein Begriff.

3.3 DATENSICHERUNG UND NOTFALLPLANUNG (LE 3)

Der Verlust wichtiger Daten – etwa durch **Diebstahl, Schadsoftware oder Bedienungsfehler** – kann für ein Unternehmen existenzbedrohend sein. Eine ausreichende Datensicherung ist daher unabdingbar.

VERTIEFUNG

Ergänzende Informationen zur Datensicherung und Notfallplanung finden Sie im Leseskript der Lerneinheit 3.

Die **Gründe für einen Datenverlust sind vielfältig**. Zu den häufigsten Ursachen gehören physikalische Einwirkungen wie Feuer, Wasser oder Überspannung. Technische Defekte, Bedienfehler wie versehentliches Löschen oder das Überschreiben von Dateien sowie kriminelle Eingriffe wie das Einschleusen von Schadsoftware können ebenfalls verantwortlich sein. Deshalb ist die regelmäßige **Datensicherung (englisch „Backup“)** ein Muss für jedes Unternehmen – egal, ob als Selbständiger, klein- bis mittelständisches Unternehmen oder Großkonzern.

Eine regelmäßige und sorgfältig geplante Datensicherung ist unerlässlich!

Ziel der Datensicherung ist es, dass alle **wichtigen Daten jederzeit wiederherstellbar sind.** Dies erfordert eine sorgfältige Planung und Durchführung. Dabei ist unter anderem festzulegen, welche Daten auf welchen Geräten wie häufig mit Hilfe welcher Software zu sichern sind. Idealerweise überträgt man die Planung und Überwachung der Datensicherung einem IT-Sicherheitsbeauftragten und bestimmt für diese Aufgabe zudem einen Stellvertreter.

Ein praktisches Hilfsmittel ist hier die **3-2-1-Regel**. Die 3 bedeutet, es werden drei Kopien gesichert (die Originaldaten zählen mit). Die 2 steht für die Lagerung der Kopien auf mindestens zwei unterschiedlichen Datenträgern. Und die 1 bedeutet, dass eine Kopie extern („offsite“, also außerhalb des Büros, der Werkstatt etc.) aufzubewahren ist.

ANREGUNG FÜR DIE SCHULUNG

Diskussion: Fragen Sie das Plenum, wer seine Daten nach dieser Regel sichert; welche alternativen Methoden werden angewandt?

Wichtig: Auch Sicherungskopien müssen vor Diebstahl oder Missbrauch geschützt werden! Den besten Schutz bietet eine entsprechende Verschlüsselung. Gute Datensicherungsprogramme bieten dies meist als Option mit an. Selbstverständlich müssen alle Schlüssel und Zugangsdaten (zum Beispiel Passwörter) für die Verschlüsselung auch gegen Verlust und Missbrauch gesichert sein.

3.4 MOBILE UND PRIVATE ENDGERÄTE AM ARBEITSPLATZ (LE 4)

Durch **Smartphones und Tablets** hat man auch unterwegs immer Zugriff auf Anwendungen und Daten. Das schließt auch Anwendungen ein, die regelmäßig für die Arbeit genutzt werden: E-Mails, Kalender, Dokumente in der Cloud und vieles mehr. Das ist praktisch und effizient, aber auch mit Risiken verbunden. Denn aus den verschiedenen App-Stores kann man sich auch Anwendungen herunterladen, die **Sicherheitslücken** aufweisen, massenhaft Daten sammeln oder im schlimmsten Fall sogar speziell für die Datenspionage/Datenmanipulation programmiert wurden. Außerdem kann ein Smartphone bzw. Tablet auch verloren gehen oder gestohlen werden, womit dann Dritte theoretisch auf alle dort gespeicherten Daten Zugriff haben.

Notwendige Sicherheitsvorkehrungen bei Smartphones und Tablets vornehmen!

Die Liste möglicher **Abwehrmaßnahmen** reicht von der Beschränkung der Rechte für die installierten Apps auf das Nötigste durch entsprechende Einstellungen im Betriebssystem über die Installation spezieller Sicherheits-Apps und die Verschlüsselung aller gespeicherten Daten bis hin zur Einrichtung einer automatischen Bildschirmsperre. Im letzten Fall wird unbefugten Dritten der Zugriff auf die gespeicherten Daten und Anwendungen so weit wie möglich erschwert. Dies gilt insbesondere dann, wenn alle auf dem mobilen Endgerät hinterlegten Daten zusätzlich noch verschlüsselt werden.

Sicherheits-Apps können – je nach Funktionsumfang – nicht nur den laufenden Schutz eines Endgeräts realisieren, sondern auch Datenzugriffe managen, eine Kindersicherung integrieren sowie Anrufe und SMS-Nachrichten blockieren.

Selbstverständlich sollte das mobile Betriebssystem stets auf dem **aktuellsten Stand** gehalten werden, um zwischenzeitlich behebbare Sicherheitslücken zu schließen.

Bei der Nutzung von öffentlichen WLAN-Hotspots können die übermittelten Daten von Dritten eingesehen werden

Eine weitere Bedrohung für mobile Endgeräte ergibt sich aus der Nutzung **ungesicherter WLAN-Verbindungen** (WLAN = Abkürzung für „wireless local area network“, bedeutet sinngemäß „drahtloses Netzwerk“), wie sie oft bei öffentlichen WLAN-Hotspots anzutreffen sind. Denn dabei kann die gesamte Kommunikation zwischen den Geräten und dem Router (der den Internetzugang herstellt) von Dritten mit der richtigen Ausrüstung mitgelesen werden. Sichere WLAN-Netze sind dagegen mit dem WPA2-Standard verschlüsselt und verlangen bei der Verbindung die Eingabe eines Passworts. Tipp: Unterwegs den Datenverkehr komplett über das Mobilfunknetz abwickeln und sicherstellen, dass sich das Mobilgerät niemals automatisch in verfügbaren WLAN-Netzen anmeldet. Am sichersten fährt man, wenn sowohl die WLAN- als auch die Bluetooth-Funktion standardmäßig deaktiviert und nur bei tatsächlichem Bedarf für die erforderliche Zeit aktiviert ist.

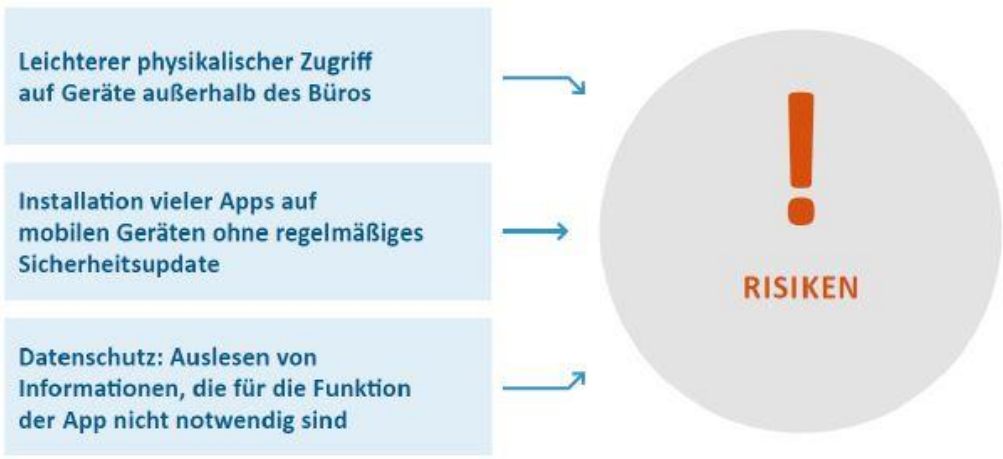
ANREGUNG FÜR DIE SCHULUNG

Stellen Sie dem Plenum Sicherheits-Apps vor!

Bedrohungen durch Smartphones und Tablets

Bei der Verwendung von privaten mobilen Endgeräten im Unternehmen, muss eine interne Sicherheitsstrategie formuliert werden.

Unsichere oder infizierte Smartphones und Tablets können für das IT-Netz eines Unternehmens eine nicht unerhebliche Bedrohung darstellen. Dürfen private mobile Endgeräte im Unternehmen genutzt werden, sollte dafür auch eine entsprechend angepasste **Sicherheitsstrategie** vorhanden sein. Dazu gehört im besten Fall eine spezielle **Mobile-Device-Management-Software** (MDM-Software), die bei allen Mitarbeiter-Geräten definierte Funktionen bereitstellt: verschlüsselte Verbindungen, 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 privaten Daten kann mit MDM-Software zudem ein professioneller Schutz erreicht werden. Diese Trennung stellt sicher, dass unsichere Apps, die auf dem Gerät installiert sind, nicht auf Systembereiche zugreifen können, die der Arbeit vorbehalten sind. Sollte eine Trennung technisch nicht umsetzbar sein, gibt es die Möglichkeit, auf privaten Geräten nur Web-Anwendungen zu nutzen, zum Beispiel Webmailer. In diesem Fall gibt es auf dem Gerät selbst nämlich keine Anwendungen oder Daten des Unternehmens. Stattdessen erfolgt dann auf dem Endgerät nur die Anzeige von Inhalten, die auf dem Server des Unternehmens liegen.



Juristische Fallstricke bei der Benutzung privater mobiler Endgeräte im Betrieb

Bei der Nutzung privater Endgeräte im Unternehmen sind bestimmte **rechtliche Vorgaben** zu beachten. So gelten für die Speicherung personenbezogener Kundendaten auf einem privaten Smartphone die gleichen Datenschutzbestimmungen wie im Unternehmen auch. Das heißt, dass ein solches Gerät beispielsweise nicht veräußert werden darf, solange sich darauf Kundendaten befinden. Wenn ein Mitarbeiter ein Gerät mit personenbezogenen Daten von Dritten verliert, muss das Unternehmen benachrichtigt werden, um es der zuständigen Datenschutz-Aufsichtsbehörde zu melden. Dazu sind alle Unternehmen gesetzlich verpflichtet, die personenbezogene Daten verarbeiten.

VERTIEFUNG

Ergänzende Informationen zum Thema „Mobile und private Endgeräte am Arbeitsplatz“ finden Sie im Leseskript der LE 4.

Augenmerk ist auch auf die nötigen **Softwarelizenzen** für die verwendeten mobilen Anwendungen zu legen. Denn viele Apps sind nur dann kostenlos, wenn man sie ausschließlich privat nutzt. Für eine unerlaubte gewerbliche Nutzung kann ansonsten das Unternehmen haftbar gemacht werden.

Nicht zuletzt gilt es auch, beim **Löschen von Unternehmensdaten** auf einem privaten mobilen Endgerät Vorsicht walten zu lassen: Unternehmen sind verpflichtet, bestimmte Unterlagen wie etwa Rechnungen aufzubewahren und zu dokumentieren. Derartige Unterlagen dürfen nicht ersatzlos gelöscht werden, auch dann nicht, wenn sie auf privaten Geräten entstehen. Geschäftsrelevante Unterlagen sollten deshalb nicht allein auf dem privaten Gerät gespeichert, sondern auch regelmäßig mit dem Unternehmensserver synchronisiert werden.

ANREGUNG FÜR DIE SCHULUNG

Zeigen Sie hier mögliche Folgen und Konsequenzen privater Nutzung mobiler Endgeräte im Unternehmen und geben Sie wenn möglich aktuelle Beispiele.

- 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

3.5 CLOUD-DIENSTE UND DATENSCHUTZ IM UNTERNEHMEN (LE 5)

Cloud-Dienste als alternativer Datenspeicher.

Onlinedienste und Cloud-Computing sind eine Alternative zum Kauf von Anwendersoftware und zum Vorhalten eigener Datenspeicher, bringen aber spezifische Risiken und Anforderungen mit sich, weil dabei die Datenspeicherung und -verarbeitung zum großen Teil außerhalb des eigenen Unternehmens erfolgen. Unterschieden werden hierbei prinzipiell folgende drei Arten von Dienstleistungen:

Unter „Cloud-Computing“ versteht man die Nutzung von durch externe Dienstleister über das Internet bereitgestellte Datenspeicher und/oder Anwendersoftware.

> **Software as a Service (SaaS):** Wird Software nicht mehr als abgeschlossenes Produkt an Endkunden verkauft, sondern über eine Cloud zu Verfügung gestellt, spricht man von Software as a Service. Konkrete Beispiele hierfür sind E-Mail-Anbieter, onlinebasierte Dokumenten-, Tabellen- und Präsentationssoftware oder Anwendungen für Unternehmen wie ein cloudbasiertes Customer-Relationship-Management-System (CRM).

> **Platform as a Service (PaaS):** Richtet sich vorwiegend an IT-Planer und -Entwickler. Über verschiedene, von Herstellern bereitgestellte Schnittstellen und Plattformen können diese eigene Programme und Anwendungen entwickeln. Dementsprechend werden über PaaS in der Regel Programmierumgebungen und Anwendungsentwicklungssysteme angeboten. Dabei haben Entwickler keinen direkten Zugriff auf die Infrastruktur, über die das jeweilige Angebot bereitgestellt wird.

> **Infrastructure as a Service (IaaS):** Hier wird von Anbietern Infrastruktur zur Verfügung gestellt, darunter vor allem Serverleistung, Rechenkapazität, Datenspeicher oder Netzwerkdienste. Die Hardware wird dabei vom Anbieter betreut, während der Kunde diese über das Internet nur steuert und nutzt.

Der Zugriff auf die Anwendungen erfolgt über das Internet

ANREGUNG FÜR DIE SCHULUNG

Stellen Sie dem Plenum bekannte Cloud-Dienste vor.

Sicherheitskriterien bei der Nutzung von Cloud-Diensten

Insbesondere bei der Speicherung unternehmenseigener Daten in einer externen Cloud – oft vereinfachend auch „Onlinespeicher“ genannt – sind im Sinne einer maximalen Sicherheit folgende **Kriterien** zu beachten:

> Werden die gespeicherten Dateien und Dokumente vor dem Hochladen in die Cloud vom Dienstanbieter verschlüsselt? Ansonsten könnten der Anbieter der Cloud oder unbefugte Dritte, die sich einen Zugang verschaffen, alle Daten einsehen.

> Ist der Zugang zum Dienst bzw. den Dokumenten mit einem Passwort versehen? Natürlich sollte auch der Zugang zum Cloud-Dienst selbst mit einem hinreichend sicheren Passwort vor Angriffen geschützt sein.

> Wo genau werden die Daten gehostet? Wo befinden sich die Server des Dienstes? Diese Frage kann eine Rolle spielen, welche Art von Daten man bei welchem Dienst aufbewahrt, um die Sicherheit vor dem Zugriff Dritter zu erhöhe, vor allem, wenn man die Daten und Dateien aus Gründen der Nutzerfreundlichkeit nicht verschlüsseln möchte.

VERTIEFUNG

Ergänzende Informationen zum Thema „Mobile und private Endgeräte am Arbeitsplatz“ finden Sie im Leseskript der LE 4.

Zusammenfassend bieten Onlinedienste und Cloud-Computing folgende **Vorteile:**

> der angemietete Online-Speicherplatz lässt sich bei Bedarf flexibel erweitern, ohne dafür neue Hardware anschaffen zu müssen,

> die Daten werden vom jeweiligen Anbieter in der Regel redundant gespeichert, was eine Datensicherung im Unternehmen selbst im Prinzip überflüssig macht,

> Cloud-Dienste sind über das Internet von unterwegs erreichbar, erlauben also auch einen problemlosen Datenzugriff bei Dienstreisen oder aus dem Homeoffice.

Dem stehen auch einige **Nachteile entgegen**. Dazu zählen:

> die Rechner-Infrastruktur eines Unternehmens steht nicht vollständig unter eigener Kontrolle. Interne Dokumente und Kundendaten können bei unzureichenden Sicherheitsmaßnahmen potenziell in falsche Hände geraten.

> Systeme, die über das Internet zugänglich sind, sind anfälliger gegen Angriffe von außen. Das bedeutet, dass Unternehmen dafür sorgen müssen, dass ihre internen Dokumente und Kundendaten etwa durch Verschlüsselung gesichert werden.

> Unternehmen begeben sich in eine Abhängigkeit vom Cloud-Anbieter (Lock-In Effekt). Gerät dieser in Schwierigkeiten, kann dies die Unternehmen, die dort Produkte nutzen, unter Umständen ebenfalls gefährden.

> Die Verantwortung für die Verarbeitung personenbezogener Daten bleibt auch bei der Beauftragung von Cloud-Dienstleistern rechtlich beim (Auftrag gebenden) Unternehmen. Daher ist besondere Sorgfalt geboten.

ANREGUNG FÜR DIE SCHULUNG

Diskutieren Sie Vor-und Nachteile von Cloud Computing und der genutzten Dienste im Plenum.

1. Ist die Ausfallsicherheit garantiert?
2. Gibt es eine Migrationsstrategie?
3. Sind die Daten durch Verschlüsselung geschützt?
4. Liegt ein Sicherheitskonzept vor?
5. Wie sieht das Berechtigungskonzept aus?

3.6. SOZIALE MEDIEN IM UNTERNEHMEN NUTZEN – ABER SICHER! (LE 6)

Fehlverhalten in sozialen Netzwerken – auch allgemein als „Social Media“ bezeichnet – kann für Unternehmen zu einem erheblichen Schaden führen, etwa in Bezug auf Reputation oder den Schutz von Betriebsgeheimnissen. Zudem können das Anbieten oder Herunterladen von Fotos, Videos und anderen Dateien schnell Urheber-, Nutzungs- und Persönlichkeitsrechte verletzen.

Prinzipiell bietet die Nutzung von Social Media den Unternehmen eine Reihe von **Potenzialen**. Dazu zählen unter anderem eine Steigerung des Bekanntheitsgrads, eine direkte Interaktion mit der Zielgruppe (zum Beispiel durch Chats oder Kommentarfunktionen), die Präsentation von Neuigkeiten (zum Beispiel in Form von Pinnwänden, Anzeigetafeln oder Terminhinweisen) und die Rekrutierung neuer Mitarbeiter.

VERTIEFUNG

Ergänzende Informationen zum Thema „Soziale Medien im Unternehmen nutzen – aber sicher!“ finden Sie im Leseskript der Lerneinheit 6.

FACEBOOK	Ermöglicht eine enge Bindung und direkte Interaktion mit Kunden, Einbindung von Texten, Fotos, Videos und Internetlinks (z.B. zur eigenen Website).
TWITTER	Empfehlenswert für kurze News, Themenrelevante Hashtags (#) sind entscheidend.
GOOGLE+	Videotelefonie, Einteilung der Kontakte in Kreise und Gruppen, Integrationsmöglichkeiten ins Google-System.
XING UND LINKEDIN	Netzwerke mit Fokus auf berufliche Kontakte, verschiedene Foren zu unternehmensrelevanten Themen.
PINTEREST	Für Branchen wichtig, bei denen Bilder eine große Rolle spielen.
INSTAGRAM	Foto-Community, persönlicher als z.B. Pinterest, eher nicht für Werbezwecke geeignet.
YOUTUBE	Vermarktung des Unternehmens/von Produkten in Videoformaten.
Snapchat	Vermarktung des Unternehmens/von Produkten in Videoformaten über Kanäle.

ANREGUNG FÜR DIE SCHULUNG

Vermutlich nutzt jeder Teilnehmer mindestens eine dieser Plattformen – verdeutlichen Sie die Risiken dieser Nutzung!

Risiken bei der Nutzung von sozialen Medien und der Weitergabe persönlicher Informationen im Unternehmen

Demgegenüber ergeben sich auch **Risiken** wie die (versehentliche) Veröffentlichung sensibler Informationen durch Datenfreizügigkeit oder Datenschutzverletzung sowie möglicherweise die Verletzung von Urheber-oder Persönlichkeitsrechten. Außerdem bieten Social-Media-Kanäle potenzielle Einfallstore für Spam, Malware und Phishing-Angriffe, um nur einige Risiken zu nennen. Deshalb sollte man sich vor der Nutzung von Social-Media-Angeboten generell fragen, welche (potenziellen) Vorteile für das Unternehmen – etwa in Bezug auf Image, Kommunikation und Umsatz – überhaupt zu erwarten sind. Weiterhin ist zu klären, welche Risiken damit verbunden sind, wenn Texte, Bilder und Videos an einen Netzwerkbetreiber abgegeben werden.

Den genannten Risiken kann man mit folgenden **Sicherheitstipps** weitgehend begegnen:

> Allgemeine Geschäftsbedingungen (AGB), Datenschutzrichtlinien und Werbeleitfäden durchlesen.

> Verwendung unterschiedlicher, sicherer Passwörter für alle Social-Media-Accounts.

> Privatsphäre-Einstellungen anpassen.

> Datensparsamkeit: Nur Informationen preisgegeben, die dauerhaft einsehbar sein dürfen.

> Über Gefahren von Phishing und Social Engineering aufgeklärt sein.

> Urheber- und Persönlichkeitsrecht bei der Verwendung von Inhalten beachten.

> Vom Hausrecht Gebrauch machen! „Melden“- und „Blockieren“-Funktion (bei Chats etc.) nutzen.

> Richtlinien des jeweiligen Seitenbetreibers bei der Veranstaltung von Gewinnspielen und Aktionen im Profil beachten.

> Ein rechtskonformes Impressum einrichten.

> Kontinuierliches Monitoring von Diskussionen und Kommentaren zum Unternehmen im sozialen Netz.

> Vorab Gedanken zum Risiko- und Krisenmanagement machen.

> Kontrollprozesse für die Pflege der Profile erarbeiten.

3.7 IT-SICHERHEIT FÜR LEITENDE IN KMU (LE 7)

Um als Betriebsleiter sicherheitsrelevante und rechtlich einzuhaltende Aspekte zu berücksichtigen, müssen nicht nur alle betreffenden Mitarbeiter für die Belange der IT-Sicherheit sensibilisiert, sondern auch zielgerichtete Präventionsmaßnahmen entwickelt werden. Nicht zuletzt kommt es darauf an, sich wirkungsvoll gegen Wirtschaftsspionage zu schützen.

Datenschutz-Grundverordnung, IT-Sicherheitsgesetz, Bundesdatenschutzgesetz

Die EU-DS-GVO regelt im Grundsatz den Schutz und den freien Verkehr personenbezogener Daten

Im Rahmen der Nutzung von IT sind zahlreiche Gesetzeswerke zu beachten. Eine große Rolle dabei spielt die **europaweit gültige Datenschutz-Grundverordnung, kurz EU-DS-GVO**. Sie ist im Mai 2016 in Kraft getreten und nach einer Übergangsfrist von zwei Jahren von Mai 2018 an anzuwenden. Das Bundesdatenschutzgesetz (BDSG) wurde im April 2017 neu verabschiedet, um das deutsche Recht an die Vorgaben der EU-DS-GVO anzupassen.

Die DS-GVO fokussiert im Grundsatz den Schutz und den freien Verkehr personenbezogener Daten und definiert in diesem Zusammenhang u.a. konkrete Rechte für Unternehmen, den einzelnen Bürger sowie Arbeitnehmer und Arbeitgeber. Zudem enthält sie Vorgaben für den Transfer von personenbezogenen Daten in Staaten außerhalb der Europäischen Union sowie Vorschriften zu Bußgeld- und Sanktionsmöglichkeiten.

VERTIEFUNG

Ergänzende Informationen zur Datenschutzgrundverordnung finden Sie ab Seite 6 des Leseskripts von Lerneinheit 7.

IT-Sicherheitsgesetz

Das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (**IT-Sicherheitsgesetz**) betrifft im Prinzip alle Betreiber kommerzieller Internetseiten, was bei den allermeisten Unternehmen der Fall ist. Es stellt bestimmte Mindestanforderungen an die technischen und organisatorischen Maßnahmen, die diese Unternehmen zum Schutz ihrer Kundendaten und ihrer IT-Systeme zu erfüllen haben. In seinem Rahmen werden außerdem die so genannten KRITIS-Verordnungen erlassen, die sich speziell an die Betreiber kritischer Infrastrukturen wie etwa Strom- und Wasserversorgungsunternehmen richten.

Ein Datenschutzbeauftragter ist gesetzlich vorgeschrieben, sobald personenbezogene Daten von mehr als neune Personen automatisiert verarbeitet werden.

Das Bundesdatenschutzgesetz (BDSG) schreibt einen **Datenschutzbeauftragten** in allen öffentlichen Stellen und Unternehmen vor, sobald **personenbezogene Daten** wie Personal- und Kundendaten **automatisiert verarbeitet werden**. Bei Unternehmen gilt diese Vorschrift in der Regel dabei erst, wenn **mehr als neun Personen** mit dieser Datenverarbeitung beschäftigt sind. Findet die Datenverarbeitung nicht automatisiert statt, greift die Vorschrift erst ab 20 Personen. Es existiert keine formale Ausbildung zum Datenschutzbeauftragten. Datenschutzbeauftragte müssen die **nötige Fachkunde und Zuverlässigkeit** mitbringen, und können an entsprechende Fort- und Weiterbildungen teilnehmen, um die Fachkunde zu erhalten.

VERTIEFUNG

Ergänzende Informationen zum Thema gesetzliche Bestimmungen und organisatorische Prävention finden Sie in Kapitel 1 und 2 des Leseskripts von Lerneinheit 7.

ANREGUNGEN FÜR DIE SCHULUNG

Gehen Sie mit der Klasse die Mindestanforderungen für Datenschutzbeauftrage durch!

Technische Präventionsmaßnahmen innerhalb der IT-Sicherheit.

Unverzichtbar sind klassische technische Präventionsmaßnahmen wie die Nutzung von **Firewall** und **Antiviren-Programmen**, die regelmäßige Datensicherung sowie die Beschränkung von Dateirechten auf das nötige Minimum. Weiterhin sollten die in vielen Soft- und Hardwareprodukten bereits herstellerseitig implementierten Schutzfunktionen aktiviert und regelmäßig **Software-Updates** durchgeführt werden. Außerdem empfiehlt es sich, alle Daten bzw. Informationen nur in verschlüsselter Form zu speichern. Bei **Passwörtern** erzielt man nach derzeitigem Stand der Technik dann ein ausreichendes Sicherheitsniveau, wenn diese aus mindestens zwölf Zeichen bestehen sowie Groß- und Kleinbuchstaben mit Ziffern und Sonderzeichen kombinieren. Ausrangierte Datenträger wie CD-ROMs, USB-Sticks oder Festplatten dürfen nicht einfach weggeworfen werden, sondern sind auf eine sichere Weise zu löschen bzw. auf eine sichere Weise unbrauchbar zu machen.

Um den Auswirkungen **rechtlicher Risiken** – beispielsweise in Form von Schadensersatzansprüchen aufgrund der Verletzung datenschutzrechtlicher Vorschriften – entgegen zu wirken, ist der Abschluss einer entsprechenden IT-Haftpflicht unbedingt zu empfehlen.

Ernennung eines Sicherheitsbeauftragten im Unternehmen.

Eine wesentliche Rolle bzgl. der IT-Sicherheit eines Unternehmens spielen die Mitarbeiter. Sie bieten wohl heutzutage noch immer die beste Versicherung gegen Sicherheitsbedrohungen aus dem Internet. Dafür müssen sie regelmäßig geschult und für sicherheitsrelevante Themen sensibilisiert werden. Hilfreich ist hier auch die Ernennung eines **Sicherheitsbeauftragten** im Unternehmen.

Beim Schutz vor **Wirtschaftsspionage** sind zwei mögliche Szenarien zu berücksichtigen: Angriffe von innen und von außerhalb. Während Zugriffsversuche von außen prinzipiell durch Sicherheitssysteme wie etwa eine Firewall erkannt bzw. verhindert werden können, ist der Schutz gegen Innentäter – dazu zählt auch vorübergehend im Unternehmen tätiges Fremdpersonal – deutlich eingeschränkt. Das liegt vor allem an möglichen Kenntnissen über vorhandene Sicherheitsvorkehrungen sowie eventuell vorhandenen Zugangs- bzw. Zugriffsberechtigungen begründet. Mögliche Ansatzpunkte sind hier die Sicherung von Räumen und/oder Gebäuden gegen unbefugten Zutritt sowie die Verschlüsselung von elektronisch gespeicherten Daten.

ABLAUFPLAN FÜR WORKSHOPS/SCHULUNGEN

6 Einheiten á 45 Minuten

Hintergrund:

Die beiliegenden Ablaufpläne für sechs Einheiten á 45 Min schlagen einen Idealverlauf einer Schulung zu IT-Sicherheitsthemen vor und können bei Bedarf (Vorwissen der Teilnehmer*innen, Teilnehmerzahl, Raumausstattung, usw.) angepasst und modifiziert werden. Unabhängig davon ist es wichtig, sich im Vorfeld als Workshopleiter*in mit den Inhalten der Schulung ausreichend auseinanderzusetzen.

Checkliste:

- ☐ Lesen Sie idealerweise die Leseskripte der Lerneinheiten 1 bis 7 oder alternativ die Zusammenfassung der Inhalte in den vorangegangenen Kapiteln. Haben Sie alle Aspekte, die Sie vermitteln möchten, verstanden?
- ☐ Planen Sie den Ablauf der Schulung: Prüfen Sie hierfür den zur Verfügung gestellten Ablaufplan. Passen die Inhalte und Methoden zu Ihrer Zielgruppe? Müssen Themen gekürzt/vertieft werden?
- ☐ Informieren Sie alle Teilnehmer*innen der Schulung rechtzeitig (im besten Fall einen Monat vor der Schulung) und bitten Sie um eine zeitnahe Bestätigung/Absage der Teilnahme.
- ☐ Gehen Sie die Anzahl der Teilnehmer*innen vor der Schulung durch und prüfen Sie die Umsetzung oder notwendige Anpassung einzelner Aufgaben und Spiele: Welche Gruppengröße bietet sich an? Wie viele Kleingruppen wird es geben?
- ☐ Organisieren Sie einen geeigneten Raum und das notwendige Equipment (Bestuhlung, PC, Beamer, Leinwand, Lautsprecher, Whiteboard/Flipchart)
- ☐ Organisieren Sie die notwendigen Schulungsmaterialien wie Lehrfilme, Präsentationsfolien und Arbeitsbögen.
- ☐ Drucken Sie notwendige Arbeitsunterlagen für die Teilnehmer*innen aus und organisieren Sie weitere notwendige Materialien (Poster, Checklisten, Requisiten für Rollenspiele etc.).
- ☐ Prüfen Sie: Ist der Foliensatz aktuell und vorhanden? Lässt sich der Lehrfilm korrekt widergeben?
- ☐ Führen Sie kurz vor der Schulung einen Technik-Check durch.

INPUT LERNEINHEIT 1: GRUNDEINSTELLUNGEN FÜR EINEN SICHEREN ARBEITSPLATZ

Thema	Inhalt und Methode	Arbeitsform	Material	Dauer
Vorbereitung	> Aufbau & ggfs. Technik-Check > Evtl. Bildung von Gruppenarbeitstischen			
Begrüßung und Einleitung	> Folie 1 (Folie nachfolgend mit F abgekürzt) Überlegen Sie sich einen geeigneten Einstieg in die Schulung, so dass sie sofort das Interesse der Teilnehmer wecken. Sie können mit einer Frage starten und so wertvolle Erkenntnisse über das Vorwissen und die Hintergründe der Teilnehmer gewinnen. Beispiele: • Welche Bedeutung besitzen neue Medien und IT in der heutigen Zeit im (eigenen) beruflichen Alltag? • Welche Rolle spielt die IT-Sicherheit in der Gesellschaft und/oder im Geschäftsalltag? > Stellen Sie den Ablauf sowie Zweck und Inhalte der Schulung kurz vor (F2). > Nur bei Lehrkräfteschulung: Stellen Sie kurz das Angebot Bottom-Up und dessen Möglichkeiten zur Einbindung in den Unterricht vor (F3).	Plenum	> Laptop oder PC > Beamer oder Smartboard > Präsentationsfolien	5 - 10 Min
Annäherung: IT-Sicherheitsrisiken	> Diskussionsfrage: Welche IT-Sicherheitsrisiken gibt es? (F4) Brainstorming mit Hilfe einer Web-Anwendung. Beispiele: https://answergarden.ch https://www.mentimeter.com Alternative: Sammlung an Tafel, Whiteboard, Flipchart etc. oder mündlich.	Plenum oder in Kleingruppen	> Smartphones/Laptops/Computer mit Internetzugang oder Tafel / Whiteboard + Stifte	5 - 10 Min
Vorstellung Schadprogramme	> Stellen Sie die Übersicht zu verschiedenen Schadprogrammen und deren Verbreitungswege vor (F5 + F6). Weisen Sie auf die Bedeutung des Themas anhand eines Beispiels hin. Vorschlag: Erfolgreiche Verbreitung von Ransomware/ Erpressersoftware wie Locky (Feb 2016) und WannaCry (Mai 2017) besonders in Unternehmen. > Austausch im Plenum: Wie kann man Schadprogrammen wie Viren und Co. vorbeugen? (F7) > Stellen Sie die Schutzfunktionen von Antivirenprogrammen und Firewall vor (F8 + F9). Verdeutlichen Sie: Nur in Kombination schützen Firewall und Antivirenschutz! Geben Sie weitere Tipps zum Schutz vor Schadsoftware (F10).	Plenum	> Laptop oder PC > Beamer oder Smartboard > Präsentationsfolien	10 Min
Vertiefung: Das sichere Passwort	> Input sichere Passwörter (F11): Machen Sie deutlich: Vielen Sicherheitsrisiken kann man mit einem sicheren Passwort vorbeugen. Verdeutlichen Sie: auch heutzutage sind die am häufigsten genutzten Passwörter „123456“ und „Passwort“. > Erklären Sie: Es gibt praktische Varianten, komplizierte Passwörter zu erstellen und sich zu merken. Geben Sie ein Beispiel einer Passphrase: 4 Frösche spielen 3 Tage lange Cello vor 2% der Pelikane = 4Fs3TlCv2%dP > Hinweis auf ergänzende Infos im Skript der LE 1, Kap. 4	Plenum	> Laptop oder PC Beamer oder Smartboard > Präsentationsfolien	5 Min
Wissenscheck	> Option 1 (bei weniger Zeit): Online-Lückentext zur LE 1 durchführen: https://www.dsin-berufsschulen.de/online-lueckentext-lerneinheit-1-grundeinstellungen-fuer-einen-sicheren-arbeitsplatz Alternativ: Lückentext als Printvariante durchführen. > Option 2 (bei mehr Zeit): Rollenspiel R1 aus LE 1 durchführen	Einzelarbeit oder in Kleingruppen Plenum	> Smartphones/Computer m. Internetzugang o. ausgedruckter Lückentext > Unterlagen Rollenspiel R1	10 - 20 Min

INPUT LERNEINHEIT 2: SICHERE DIGITALE KOMMUNIKATION IM BERUFLICHEN KONTEXT

Thema	Inhalt und Methode	Arbeitsform	Material	Dauer
Vorbereitung	> Aufbau & ggfs. Technik-Check > Evtl. Bildung von Gruppenarbeitstischen			
Begrüßung und Einleitung	> Kurz das Thema einleiten: Digitale Kommunikation im betrieblichen Alltag (F12) > Z.B. mit einer Diskussionsfrage: • Welche Kommunikationskanäle werden im Unternehmen genutzt? Welche davon intern und welche in der Außenkommunikation und Öffentlichkeitsarbeit? • Welche Risiken muss man bei der Nutzung von digitalen Kommunikationsmitteln beachten?	Plenum	> Laptop oder PC > Beamer oder Smartboard > Präsentationsfolien	5 - 10 Min
Bearbeitung Lehrfilm LE2: E-Mail Sicherheit im betrieblichen Kontext	> Zeigen des Lehrfilms LE2: E-Mail Sicherheit im betrieblichen Kontext > An gekennzeichneten Stellen den Film pausieren und in Kleingruppen oder im Plenum die Fragen beantworten: • Welche Vorkehrungen sind für eine sichere E-Mail Kommunikation für Unternehmen sinnvoll? • Was sollte man als Mitarbeiter*in beachten? > Brainstorming mit Hilfe einer Web-Anwendung. Beispiele: https://answergarden.ch https://www.mentimeter.com > Alternative: Sammlung an Tafel, Whiteboard, Flipchart etc. oder nur mündlicher Austausch der Ergebnisse im Plenum > Film zu Ende schauen, offene Fragen klären	Plenum oder in Kleingruppen	> Laptop oder PC mit Internetzugang > Beamer + Soundsystem oder Smartboard > Lehrfilm LE2: E-Mail Sicherheit im betrieblichen Kontext	15 - 20 Min
Risiken & Schutzmaßnahmen bei digitaler Kommunikation	> Erläuterung von Risiken und Schutzmaßnahmen bei der digitalen Kommunikation (F13 – F16) > Erklären Sie hier unbedingt vertiefend die Begriffe Phishing und Social Engineering! Hier können Sie den Teilnehmern den Auftrag geben, mal ihren Spam-Ordner zu sichten und zu schauen, wie viele Emails von den verschiedensten Absendern im Ordner liegen (natürlich OHNE die Mails zu öffnen!) > Maßnahmen zur Vorbeugung vorstellen. Gehen Sie hier auf die unterschiedlichen Signaturmöglichkeiten ein und die damit verbundene Vermeidung von Phishing. > Thema Datenschutz bei digitaler Kommunikation (F17): Erklären Sie hier genau die Bedeutung von Adressat, CC und BCC. Möglichweise haben mehrere Teilnehmer noch nicht so viele (oder gar keine) berufliche Email verfassen müssen.	Plenum	> Laptop oder PC > Beamer oder Smartboard > Präsentationsfolien	10 Min
Wissenscheck	> Online-Quiz zur LE 2 durchführen www.dsin-berufsschulen.de/unsere-online-quiz > Alternativ: Quiz als Printvariante durchführen.	Einzelarbeit oder in Kleingruppen	> Smartphones/Computer mit Internetzugang > oder Quizbögen Q2 aus LE2	10 Min

INPUT LERNEINHEIT 3: DATENSICHERUNG UND NOTFALLPLANUNG FÜR UNTERNEHMEN

Thema	Inhalt und Methode	Arbeitsform	Material	Dauer
Vorbereitung	> Aufbau & ggfs. Technik-Check > Evtl. Bildung von Gruppenarbeitstischen			
Begrüßung und Einleitung	> In das Thema einleiten: Datensicherung und Notfallplanung für Unternehmen (F18) > Z.B. mit Diskussionsfrage: Welche Arten von Daten gibt es im Unternehmen? Welche davon sind „lebenswichtig“? > Vergleich mit Folie 19: Schutz aller Unternehmensdaten	Plenum	> Laptop oder PC > Beamer oder Smartboard > Präsentationsfolien	5 Min
Gründe für Datenverlust	> Erläuterung Gründe für Datenverlust (F20) Weisen Sie darauf hin: Einflussfaktoren sind nie absehbar (Naturkatastrophen, beschädigte Festplatte, Virus) und daher muss die Datenspeicherung regelmäßig, in kurzen Abständen, erfolgen.	Plenum	> Laptop oder PC > Beamer oder Smartboard > Präsentationsfolien	5 Min
Bearbeitung Lehrfilm LE3: Datensicherung & Notfallplanung	> Zeigen des Lehrfilms: www.youtube.com/watch?v=J5qG1KKqna4 > An gekennzeichneten Stellen den Film pausieren und in Kleingruppen oder im Plenum die Fragen beantworten: • Welche Maßnahmen sind für Unternehmen hinsichtlich einer zuverlässigen Datensicherung sinnvoll? • Worauf sollten Mitarbeiter*innen bei der Datensicherung achten? > Brainstorming mit Hilfe einer Web-Anwendung. Beispiele: https://answergarden.ch https://www.mentimeter.com > Alternative: Sammlung an Tafel, Whiteboard, Flipchart etc. oder nur mündlicher Austausch der Ergebnisse im Plenum > Film zu Ende schauen, offene Fragen klären	Plenum oder in Kleingruppen	> Laptop oder PC mit Internetzugang > Beamer + Soundsystem oder Smartboard > Lehrfilm LE3: Datensicherung & Notfallplanung	15 - 20 Min
Planung und Durchführung Datensicherung	> F21: Weisen Sie auf die Dringlichkeit und Aktualität des Themas Datensicherung hin! Auch hier der Hinweis der Bedeutung einer regelmäßigen Datensicherung als Präventionsmaßnahme gegen die Folgeschäden eines Befalls durch Erpressersoftware! Weisen Sie auf eine sorgfältige Planung hin. > Geben Sie wichtige Hinweise zur Umsetzung (F22): Anregung: Fragen Sie das Plenum, was es von der Benennung eines Sicherheitsbeauftragen hält und ob es solch eine Person bereits ihn ihrem Unternehmen gibt. Wichtige Unterlagen sollten mehrfach gespeichert und an verschiedenen Orten gelagert werden. > Stellen Sie die 3-2-1 Regel vor (F23). > Geben Sie weitere Tipps für eine gute Datensicherung (F24).	Plenum	> Laptop oder PC > Beamer oder Smartboard > Präsentationsfolien	5 - 10 Min
Wissenscheck	> Online-Quiz zur LE 3 durchführen www.dsin-berufsschulen.de/unsere-online-quiz > Alternativ: Quiz als Printvariante durchführen.	Einzelarbeit oder in Kleingruppen	> Smartphones/Computer mit Internetzugang > oder Quizbögen Q3 aus LE3	10 Min

INPUT LERNEINHEIT 4: MOBILE UND PRIVATE ENDGERÄTE AM ARBEITSPLATZ

Thema	Inhalt und Methode	Arbeitsform	Material	Dauer
Vorbereitung	> Aufbau & ggfs. Technik-Check > Evtl. Bildung von Gruppenarbeitstischen			
Begrüßung und Einleitung	> Begrüßung und Diskussionsfrage im Plenum (F25+F26): Dieses Thema ist sehr aktuell und bietet vermutlich den größten Diskussionsbedarf. Sie können daher gut mit einer Frage in die Stunde einsteigen, Z.B.: • Nutzen Sie ein dienstliches oder privates Smartphone für die Arbeit? • Für welche Zwecke?	Plenum	> Laptop oder PC > Beamer oder Smartboard > Präsentationsfolien	5 Min
Annäherung BYOD	> Erläuterung des Begriffs BYOD und Herausforderungen (F27) > Austausch im Plenum: • Was sind die Vor- und Nachteile von BYOD? • Welche Risiken müssen bei der Nutzung von Smartphones und Tablets im betrieblichen Kontext beachtet werden?	Plenum	> Laptop oder PC > Beamer oder Smartboard > Präsentationsfolien	5 Min
Bearbeitung Lehrfilm LE4: Mobile und private Endgeräte am Arbeitsplatz	> Zeigen des Lehrfilms LE4: Mobile und private Endgeräte am Arbeitsplatz > An gekennzeichneten Stellen den Film pausieren und im Plenum die Fragen diskutieren: • Was kann man tun, um sein mobiles Gerät und die Daten zu sichern? • Welche Besonderheiten müssen dabei am Arbeitsplatz beachtet werden? > Abspielen des restlichen Films bis zu den weiteren Fragen, diese ebenfalls im Plenum besprechen: • Was hätte Betty besser machen können, um den Schaden zu vermeiden? • Worauf hätte sie besonders achten sollen? > Film zu Ende schauen, offene Fragen klären	Plenum	> Laptop oder PC mit Internetzugang > Beamer + Soundsystem oder Smartboard > Lehrfilm LE4: Mobile und private Endgeräte am Arbeitsplatz	15 - 20 Min
Vertiefung: Risiken und Schutzmaßnahmen BYOD	> Thematisierung IT-Sicherheitsrisiken (F28) Eindeutig auf alltägliche Gefahren des Smartphones hinweisen! Fragen Sie die Teilnehmer nach aktuellen Beispielen! Welche Risiken müssen bei der Nutzung beachtet werden? > Erläuterung Sicherheitsmaßnahmen (F29 – F32): Die Teilnehmer können an dieser Stelle die Einstellungen des Smartphones überprüfen und versuchen herauszufinden, welche Maßnahmen sie ergreifen können. > Hinweis auf ergänzende Infos im Skript der LE 4	Plenum	> Laptop oder PC > Beamer oder Smartboard > Präsentationsfolien	10 Min
Wissenscheck	> Online-Quiz zur LE 4 durchführen www.dsin-berufsschulen.de/unsere-online-quiz > Alternativ: Quiz als Printvariante durchführen.	Einzelarbeit oder in Kleingruppen	> Smartphones/Computer mit Internetzugang > oder Quizbögen Q4 aus LE4	10 Min

INPUT LERNEINHEIT 5: CLOUD-DIENSTE UND DATENSCHUTZ UND LERNEINHEIT 6: SOZIALE MEDIEN IN UNTERNEHMEN NUTZEN – ABER SICHER!

Thema	Inhalt und Methode	Arbeitsform	Material	Dauer
Begrüßung und Einleitung Cloud-Dienste	> Leiten Sie in das Thema Cloud-Dienste ein und fragen Sie die Teilnehmer, ob ihnen der Begriff bekannt ist (F33 – F34). Erklären Sie kurz relevante Informationen.	Plenum	> Laptop oder PC > Beamer oder Smartboard > Präsentations-folien	5 Min
Potentiale und Risiken von Cloud-Diensten	> Austausch im Plenum (F35): Welche Potentiale sowie Risiken bietet die Nutzung von Cloud-Diensten in Unternehmen? Vergleich mit Folie 36 > Erläuterung Sicherheitsmaßnahmen (F37) Hier lassen sich noch weitere Maßnahmen formulieren. Fragen Sie die Teilnehmer danach! Beispiele: Wie lange stehen die Daten zur Verfügung? Welche Server werden zur Speicherung verwendet? Sind die Daten von überall und jederzeit abrufbar? Darf nur eine bestimmte Anzahl von Endgeräten auf die Cloud zugreifen? > Die Cloud-Anbieten müssen sich an strengste Sicherheitsvorkehrungen halten. Sensibilisieren Sie die Teilnehmer hier noch einmal zum Abschluss des Themas, Cloud-Dienste mit Bedacht auszuwählen und zu nutzen. > Verdeutlichen Sie in diesem Zusammenhang das Thema Datenschutz (F40)	Plenum	> Laptop oder PC > Beamer oder Smartboard > Präsentations-folien	10 Min
Einleitung: Potentiale und Risiken von Sozialen Netzwerken	> Austausch im Plenum (F39 + F40): Welche sozialen Netzwerke nutzen die Teilnehmer privat und ihre Unternehmen beruflich? Welche Potentiale sowie Risiken bietet der Einsatz von Social Media für Unternehmen?	Plenum	> Laptop oder PC > Beamer oder Smartboard > Präsentations-folien	5 - 10 Min
Bearbeitung Lehrfilm LE6: Social Media im betrieblichen Kontext	> Zeigen des Lehrfilms LE6: Social Media im betrieblichen Kontext > An gekennzeichneten Stellen den Film pausieren und im Plenum die Fragen diskutieren: • Was hat Robert hier falsch gemacht? • Was sollten Mitarbeiter unbedingt bedenken, bevor sie Inhalte veröffentlichen? > Abspielen des restlichen Films bis zu den weiteren Fragen, diese ebenfalls im Plenum besprechen: • Was hätten Herr Meier und Robert hier beachten müssen? • Was sollte grundsätzlich im Umgang mit Social Media gelten? > Film zu Ende schauen, offene Fragen klären	Plenum	> Laptop oder PC mit Internetzugang > Beamer + Soundsystem oder Smartboard > Lehrfilm LE6: Social Media im betrieblichen Kontext	15 - 20 Min
Zusammenfassung und Schlussfolgerung für Unternehmen	> Fassen Sie noch einmal die Risiken von Sozialen Netzwerken und der Urheberrechtsverletzung kurz zusammen bzw. gehen Sie nur noch einmal auf die Punkte ein, die noch nicht genannt wurden (F41 + F42) Besonders wichtig sind hier vor allem die Sicherheits- bzw. Privatsphäre-Einstellungen. Unternehmen dürfen nur Informationen veröffentlichen, für welche sie auch die Lizenzen besitzen! Appellieren Sie an die Teilnehmer, ihre Geschäftsführer und leitenden Personen im eigenen Unternehmen darauf hinzuweisen! > Gehen Sie zusammen die Regeln zum sicheren Umgang	Plenum	> Laptop oder PC > Beamer oder Smartboard > Präsentations-folien	5 - 10 Min

	mit Sozialen Netzwerken durch (F43 - F45). > Hinweis auf ergänzende Infos im Skript der LE 6			
Optional: Wissenscheck	> Wenn noch Zeit ist: Lückentext aus LE 6: https://www.dsin-berufsschulen.de/online-lueckentext-le-6 > Alternativ: Lückentext als Printvariante durchführen.	Einzelarbeit oder in Kleingruppen	> Smartphones/Computer m. Internetzugang o. ausgedruckter Lückentext	5 - 10 Min

INPUT LERNEINHEIT 7: IT-SICHERHEIT FÜR LEITENDE IN KLEINEN UND MITTLEREN UNTERNEHMEN

Thema	Inhalt und Methode	Arbeitsform	Material	Dauer
Vorbereitung	> Aufbau & ggfs. Technik-Check > Evtl. Bildung von Gruppenarbeitstischen			
Begrüßung und Einleitung: Informationssicherheit	> Leiten Sie in das Thema ein: Fragen Sie danach, wer sich in kleinen und mittleren Unternehmen meist um IT und IT-Sicherheit kümmert? Stellen Sie die Verantwortung eines Betriebsleitenden für IT-Sicherheit heraus (F46). > Fragen Sie die Teilnehmer, ob ihnen der Begriff Informationssicherheit bekannt ist und was sie darunter verstehen. Erläutern Sie die vier Aspekte der Informationssicherheit (F47).	Plenum	> Laptop oder PC > Beamer oder Smartboard > Präsentationsfolien	10 - 15 Min
Input: persönliche Haftung von Geschäftsführenden	> Gehen Sie auf die persönliche Haftung von Geschäftsführenden, insb. auf die Notwendigkeit eines Datenschutzbeauftragten sowie die Maßnahmen zum Schutz vor Schadensansprüchen ein (F48 – F50).	Plenum	> Laptop oder PC > Beamer oder Smartboard > Präsentationsfolien	5 Min
Input: Gesetzliche Bestimmungen	> Option 1 (bei weniger Zeit): Erläutern Sie die wichtigsten Punkte der Datenschutzgrundverordnung (F51) sowie des IT-Sicherheitsgesetzes (F52). > Option 2 (bei mehr Zeit): Bildung von Kleingruppen und Bearbeitung des Arbeitsbogens AB 7B „Gesetzliche Bestimmungen“. Präsentation der Ergebnisse im Plenum und Besprechung der Frage: Welche Schlussfolgerungen im Hinblick auf die Mitarbeiter sollte man als Betriebsleiter ziehen? (dazu können Folie 56 + 57 gezeigt werden).	Plenum Kleingruppen	> Laptop oder PC > Beamer oder Smartboard > Präsentationsfolien	5 -10 Min 15 - 20 Min
Input: Präventionsmaßnahmen	> Austausch im Plenum zur Diskussionsfrage (F53): Was sollte man als Betriebsleitende*r hinsichtlich seiner Mitarbeiter beachten, um die IT-Sicherheit im Betrieb zu verbessern? > Erläutern Sie die technisch-organisatorischen Maßnahmen „Mitarbeiterschulung“ sowie „IT-Sicherheitsbeauftragte/r“ und stellen Sie das Konzept einer Sicherheitsleitlinie vor (F54 – F56). > Erläutern Sie das Thema Wirtschaftsspionage im Zusammenhang mit der IT-Sicherheit (F57 – F58). > Hinweis auf ergänzende Infos in Skript der LE 7	Plenum	> Laptop oder PC > Beamer oder Smartboard > Präsentationsfolien	5 - 10 Min
Optional: Wissenscheck	> Wenn noch Zeit ist: Online-Quiz zur LE 7 durchführen www.dsin-berufsschulen.de/unsere-online-quiz > Alternativ als Printversion	Einzelarbeit oder in Kleingruppen	> Smartphones/Computer m. Internetzugang o. ausgedruckter Lückentext	5 - 10 Min

INPUT UMSETZUNG DES LEHRANGEBOTS BOTTOM-UP IM UNTERRICHT

Thema	Inhalt und Methode	Arbeitsform	Material	Dauer
Vorbereitung	> Aufbau & ggfs. Technik-Check > Evtl. Bildung von Gruppenarbeitstischen			
Begrüßung und Einleitung: Ziel und Zweck von Bottom-Up	> Stellen Sie kurz Ziel und Zweck von Bottom-Up vor (F59 – F60) sowie die sieben Lerneinheiten (F61). > Erläutern Sie, was jede Lerneinheit enthält (F62).	Plenum	> Laptop oder PC mit Beamer oder Smartboard	5- 10 Min
Input: Die Nutzung des Angebots im Unterricht	> Gehen Sie die einzelnen Schritte durch, die zur Nutzung und Umsetzung des Angebots notwendig sind (F63). Hierzu kann auch parallel die Projektwebseite aufgerufen und vorgestellt werden. > Erklären Sie die Arten der Leistungskontrolle (F64) und erläutern Sie die damit verbundenen Möglichkeiten, die Inhalte von Bottom-Up als Prüfungsstoff zu behandeln. > Geben Sie einen exemplarischen Einblick in die Materialien und teilen Sie diese wenn möglich aus.	Plenum	> Laptop oder PC, wenn möglich mit Internetzugang > Beamer oder Smartboard > Präsentationsfolien > Materialien zur Ansicht, ausgedruckt oder digital	10 - 15 Min
Input: Gestaltung der Transfersituation	> Erklären Sie: Nach Behandlung im Unterricht wenden die SuS mit Hilfe eines Arbeitsauftrags und passenden Transfermaterialien ihr Wissen im Betrieb an und geben es an Kollegen weiter. Nach Erfüllung des Arbeitsauftrags händigen die Lehrkräfte den SuS Teilnahmebescheinigungen aus, die sie online generieren können. Diese Funktion können Sie live auf der Projektwebseite zeigen. > Zeigen Sie exemplarisch ein paar Transfermaterialien.	Plenum	> Laptop oder PC, wenn möglich mit Internetzugang > Beamer oder Smartboard > Präsentationsfolien > Materialien zur Ansicht, ausgedruckt oder digital	5 - 10 Min
Abschluss	> Offene Fragen klären > Nach Feedback fragen: Fragen Sie das Plenum nach Feedback! Was war gut, was fanden sie nicht so gut? Was hätten sie sich noch gewünscht? > Teilen Sie Informationsmaterial von Bottom-Up aus; z.B. die Handreichung zur Umsetzung von Bottom-Up und/oder den Projektbericht > Sie können am Ende der Schulung eine Teilnehmerliste (mit Kontaktdaten) herumgeben, z.B. für den weiteren konstruktiven Austausch unternehmensübergreifend in der Zukunft.	Plenum	> Informationsmaterial von Bottom-Up	5 - 10 Min

NOTIZEN

PLATZ FÜR ANMERKUNGEN UND IDEEN

NOTIZEN

PLATZ FÜR ANMERKUNGEN UND IDEEN

NOTIZEN

PLATZ FÜR ANMERKUNGEN UND IDEEN

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.

www.dsin-berufsschulen.de