LEHRERMAPPE

LESESKRIPT & UNTERRICHTSMATERIAL

Berufsschüler BOTTOM-UP! für IT-Sicherheit

LERNEINHEIT 3: DATENSICHERUNG & NOTFALLPLANUNG

Heutzutage nutzt grundsätzlich jedes Unternehmen Computer und Smartphones, um seine Geschäftsvorgänge zu verwalten. Ein **Verlust der Daten**, etwa durch Diebstahl, Schadsoftware oder Bedienungsfehler, kann **existenzbedrohend für das Unternehmen** sein. Eine **ausreichende Datensicherung** ist daher unabdingbar.

DIE THEMEN:

Für welche Ausbildungslehrgänge empfohlen?

Diese Lerneinheit wird **übergreifend für alle Ausbildungslehrgänge**, doch vor allem für Auszubildende **kaufmännischer** und **informationstechnischer Ausbildungslehrgänge** empfohlen.

LERNZIELE

Nach diesen Unterrichtseinheiten wissen die Schüler*:

- ✓ wie wichtig der Schutz der Daten vor Verlust für das Unternehmen ist,
- ✓ wie man schrittweise eine Datensicherung plant und durchführt,
- ✓ was man dafür beachten sollte.

*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. DATENVERLUST: URSACHEN UND FOLGEN

Es gibt nahezu kein Unternehmen, das ohne Computer oder Smartphone arbeitet. Zentral sind hier die auf den Geräten gespeicherten Daten.

ANREGUNGEN FÜR DEN UNTERRICHT

Diskussionsfrage: Welche Arten von Daten gibt es im Unternehmen? Welche sind davon „lebenswichtig“?

Die Gründe für Datenverlust können vielfältig sein: Physikalische Einwirkungen, Hardwarefehler, Bedienfehler, Diebstahl, Schadsoftware.

Zu diesen Daten gehören **Geschäftsdokumente** wie Rechnungen und Angebote, **Personal**- und **Buchhaltungsdatenbanken**. Die interne und externe Kommunikation wird häufig per **E-Mail** und **Messaging** abgewickelt. **Zugangsdaten** oder **Registrierungscodes** werden auf PCs, Laptops und Smartphones gespeichert.

Ein Datenverlust kann für ein Unternehmen existenzbedrohend sein. Es kann seinen Verpflichtungen gegenüber Kunden, Lieferanten, Banken und Behörden nicht mehr nachkommen. Ohne Daten kann ein Unternehmen nicht überleben.

Die Gründe für einen Datenverlust können vielfältig sein. Zu den häufigsten Ursachen gehören:

> **Physikalische Einwirkungen**: Brand, Wasserschäden, Überspannung, etc.

> **Technische Fehler:** bei Festplatten kann durch Alter oder Defekt ein irreparabler Fehler auftreten. Auch Software kann z.B. durch **Fehlkonfiguration ein Grund für Datenverlust sein.**

> **Menschliche Fehler:** Mitarbeiter können durch versehentliches **Löschen** oder das **Überschreiben** von Dateien genauso zu einem Datenverlust beitragen. Hier ist die **Vergabe** von Berechtigungen eine wichtige Präventionsmaßnahme. Datenverlust kann auch durch den Verlust von Handy oder Laptops geschehen, genauso bei **Beschädigungen** an den Geräten durch Erschütterungen/Herunterfallen.

Cyberkriminelle fordern durch Erpressersoftware Lösegeld für die Freigabe der Daten.

> **Kriminelle Eingriffe:** natürlich können Geräte durch Diebe auch **entwendet** werden. Kriminelle Eingriffe erfolgen mittlerweile oft auch über das **Einschleusen von Schadsoftware**: beispielsweise kann sich durch Phishing-E-Mails sogenannte Erpressersoftware auf dem Rechner installieren, die die Daten für den Nutzer durch Verschlüsselung unbrauchbar macht (Siehe hierzu auch Lerneinheiten 1: *Grundeinstellungen für einen sicheren Arbeitsplatz* und Lerneinheit 2: *Sichere digitale Kommunikation im betrieblichen Kontext*).

ANREGUNGEN FÜR DEN UNTERRICHT

Fragen Sie die Schüler: Wie können Daten verloren gehen? Lassen Sie eine Liste erstellen. Anschließend wird diese mit der Liste in „Datensicherung“ bei Wikibooks vergleichen.

https://de.wikibooks.org/wiki/Datensicherung/_Risiken

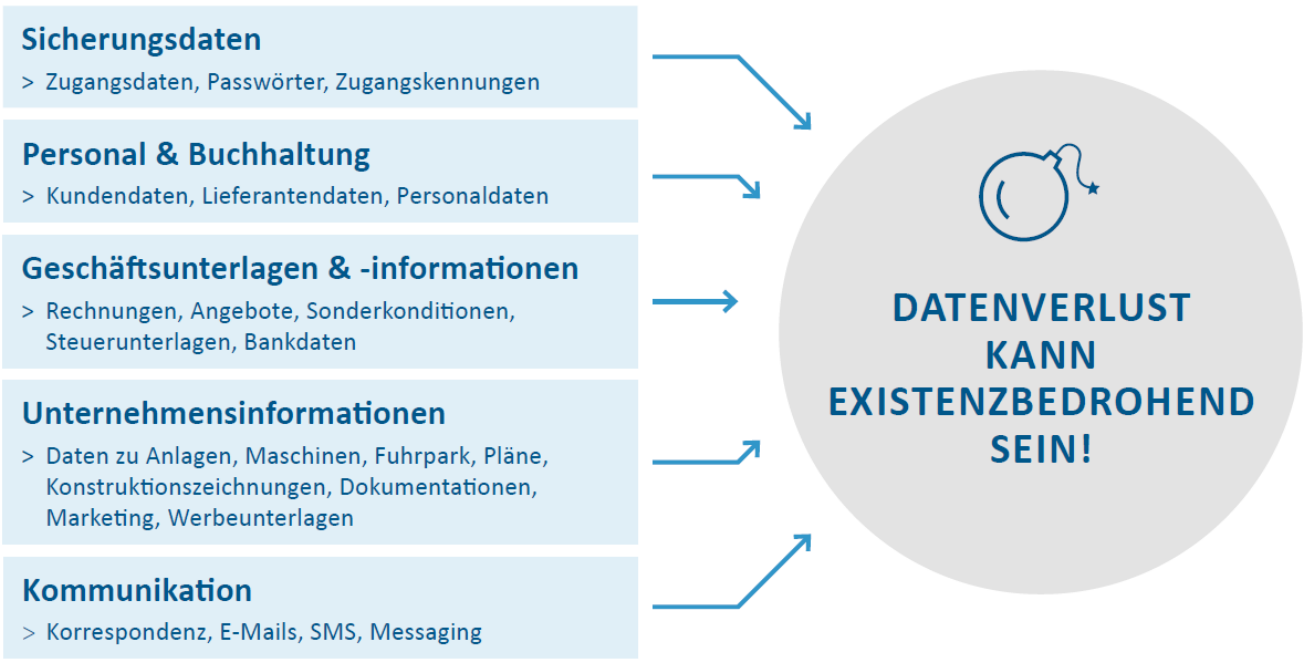
Jeder Datenverlust im Unternehmen kann viel Zeit und Geld kosten. Das Wiederherstellen nur **einer** Festplatte, die nicht gesichert wurde, kann bis zu mehreren **Tausend Euro** kosten **–** ohne Garantie, dass die Daten wiederherstellt werden können.

Verlust von Daten kann Konkurs für das Unternehmen zur Folge haben.

Trotzdem versäumen viele Unternehmen, ihre Daten **ausreichend zu sichern**. Die Gründe dafür sind unterschiedlich: Der Preis, technische Unwissenheit, zusätzliche – störende – Abläufe im Produktionsablauf und vieles mehr. Immer wieder hört man: „Mir kann das nicht passieren.“ Unternehmen bedenken nicht, wie teuer, zeitaufwendig oder gar unmöglich es ist, gelöschte, gestohlene oder verloren gegangene Daten wieder herzustellen.

Datensicherung ist wichtig für jedes Unternehmen, unabhängig von der Größe.

Eine **Datensicherung** (englisch „**Backup**“) ist **ein Muss für jedes Unternehmen**, egal ob als Selbständiger, klein- bis mittleren Unternehmen oder Großkonzern.



2. EINE DATENSICHERUNG IM UNTERNEHMEN EINFÜHREN

Datensicherung muss geplant werden.

Ziel einer ausreichenden Datensicherung ist es, dass **alle wichtigen Daten jederzeit wiederherstellbar sind**. Hat man eine Datei versehentlich gelöscht, kann man sie aus einer Sicherungskopie wiederherstellen. Wenn ein Computer **gestohlen oder zerstört** wurde, ist es möglich, alle Daten aus Sicherungskopien auf einen neuen Computer zu kopieren. Dies erfordert eine sorgfältige Planung und Durchführung. Im laufenden Betrieb sollte die Hauptarbeit nur darin bestehen, die Sicherungskopien regelmäßig zu überprüfen.

IT-Sicherheitsbeauftragte benennen

Die Datensicherung muss sorgfältig geplant und durchgeführt werden – und zwar regelmäßig. Dazu gehört, dass es verantwortliche Personen gibt, die im Notfall wissen, was zu tun ist. Hierzu benennt das Unternehmen einen IT-Sicherheitsbeauftragten sowie einen **Stellvertreter**. Diese **planen** und **setzen** die Datensicherung um. Sie **überwachen** den laufenden Betrieb und **helfen im Notfall**. Ist der Verantwortliche nicht erreichbar, hat der **Stellvertreter** die notwendigen Informationen, um die Daten wiederherstellen zu können.

ANREGUNGEN FÜR DEN UNTERRICHT

Lassen Sie die Schüler im Unternehmen nachfragen: Wer ist verantwortlich für die Datensicherung? Gibt es einen Stellvertreter?

Datensicherung planen

Für eine sorgfältige Planung werden als erstes **alle Daten und Geräte aufgelistet**, die gesichert werden müssen. Wichtig ist, **alles vollständig zu erfassen**. Dann wird für jede dieser Daten und Geräte **festgelegt, wie sie gesichert** werden:

> Von welchem Gerät auf welchen Datenträger?

> Wie häufig sichern (wie oft, an welchen Tagen, zu welcher Tageszeit)?

> Mit welchem Sicherungsprogramm? Mit welchen Einstellungen?

> Was geschieht automatisch, was muss ein Mitarbeiter tun?

WIEVIELE DATENKOPIEN SIND NOTWENDIG?

Ein praktisches Hilfsmittel ist hier die **3-2-1-Regel**:

3: Es werden **drei Kopien** gesichert (die Originaldaten zählen mit).

2: Diese sind auf mindestens **zwei unterschiedlichen Datenträgern** gelagert.

1: **Eine Kopie wird extern** (offsite – außerhalb des Büros, der Werkstatt usw.) aufbewahrt.

BEISPIEL 3-2-1-REGEL

Die Daten auf einem Laptop (**erste** Kopie) werden regelmäßig auf einem angeschlossenen USB-Stick kopiert (**zweite** Kopie). Sobald der Laptop mit dem Internet verbunden ist, wird außerdem eine weitere (**dritte**) Kopie der Daten extern (offsite) bei einem Cloud-Dienst gespeichert (Welche Cloud-Dienste hierfür geeignet sind vermittelt Lerneinheit 5).

Datensicherung muss dokumentiert werden.

Wichtig: Alles dokumentieren

Nicht immer ist der Verantwortliche für die Datensicherung erreichbar. Daher muss alles in einer **Dokumentation schriftlich festgehalten** werden. Damit kann dann der Vertreter, ein anderer Mitarbeiter oder ein externer Experte nachvollziehen, wie die Datensicherung im Unternehmen funktioniert.

TIPP

Drucken Sie die Dokumentation auf **Papier** aus. So ist sie verfügbar, auch wenn alle Computer ausgefallen sind.

Heben Sie die Dokumentation an einem **sicheren Ort** auf. So geht sie zum Beispiel bei einem Brand nicht verloren und Kriminelle können die Informationen nicht missbrauchen.

Plan umsetzen

Datenträger und Software zur Sicherung müssen angeschafft werden.

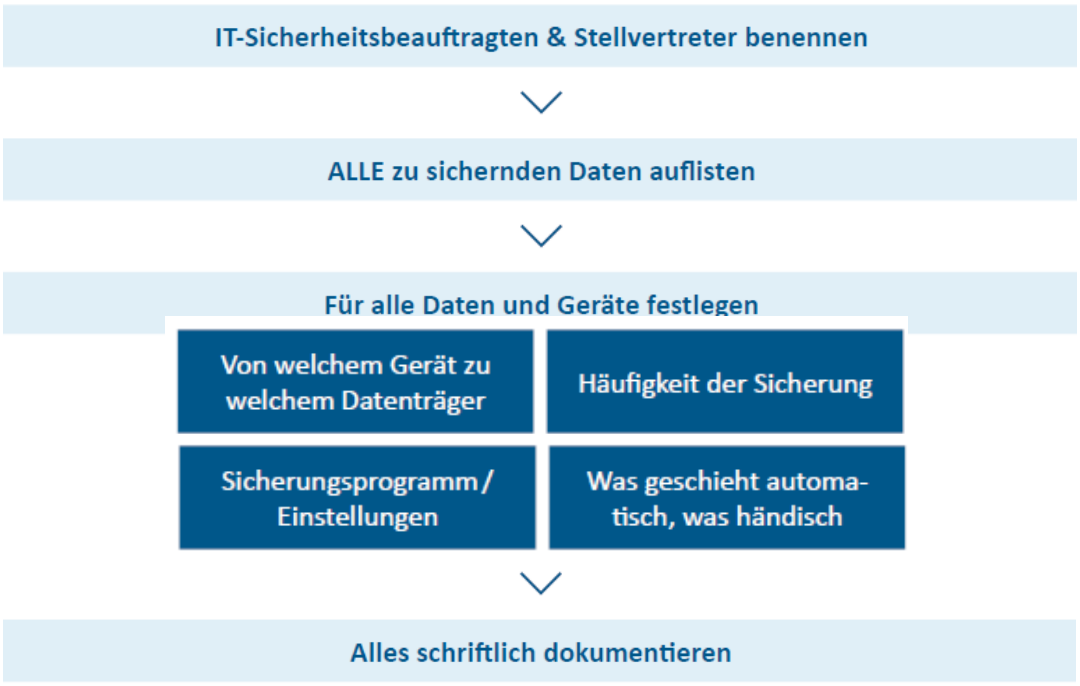
Der fertige Plan wird nun umgesetzt: Datenträger und Software werden angeschafft und installiert. Eine wichtige Aufgabe ist, die **Mitarbeiter ausreichend einzuweisen**. Dies ist ein wichtiger Teil einer Datensicherung. Denn einige Arbeiten sind nicht automatisierbar, zum Beispiel die externe Festplatte an den Computer zu schließen, oder den Datenträger an einen sicheren Ort zu transportieren.

Regelmäßig die Sicherungskopien überprüfen

Wer Daten nur sichert, hat das Wichtigste vergessen: Man muss **regelmäßig überprüfen**, ob die Daten auf den **Sicherungskopien** auch **wiederherstellbar** sind.

BEISPIEL

Der Freiberufler Otto Brucke brennt seit Jahren täglich alle wichtigen Daten auf DVDs und hebt sie in seinem Banktresor auf. Eines Tages zerstört ein Virus seine Daten. Als er seine Daten von den letzten DVDs wiederherstellen möchte, stellt er fest: Keine der DVDs lässt sich lesen! Der IT-Sicherheitsbeauftragte Jens Unger eines kleinen Unternehmens ist schlauer: An jedem ersten Freitag im Monat wählt der IT-Sicherheitsbeauftragte einige Dokumente, eine Datenbank oder andere Daten aus. Er liest sie aus der Sicherungskopie ein und überprüft sie. Stimmen sie mit den aktuellen Daten überein, dann funktioniert die Datensicherung korrekt.



3. MAßNAHMEN FÜR EINE GUTE DATENSICHERUNG

Eine Datensicherung ist wie eine **Versicherung**: Sie kostet Zeit und Geld, aber man weiß nicht, wann und ob man sie brauchen wird. Daher möchte man so wenig wie möglich dafür ausgeben, aber im Schadensfall so viel wie möglich zurückbekommen.

Eine perfekte Datensicherung gibt es nicht. Man kann nur **Risiken minimieren**. Die folgenden Tipps helfen dabei, eine ausreichende Datensicherung für ein Unternehmen zu erstellen.

Datensicherung automatisieren

Datensicherungsprogramme unterstützen!

Kein Mitarbeiter hat die Zeit, sich ständig mit dem Sichern seiner Daten zu beschäftigen. Eine gute Datensicherung lässt **so viel wie möglich automatisch** von dem eingesetzten Datensicherungsprogramm erledigen.

BEISPIEL

Bisher musste Hubert Kaufmann für jede Datensicherung die externe Festplatte anschließen, dann das Datensicherungsprogramm starten und die zu sichernden Daten angeben. Das war lästig und zeitaufwendig. Irgendwann war seine „neueste“ Datenkopie acht Monate alt. Das neue Datensicherungsprogramm erinnert ihn täglich um 17 Uhr daran, die Festplatte anzuschließen, und sichert dann automatisch alle wichtigen Daten. Am Ende erhält Hubert Kaufmann die Meldung, dass alles gesichert wurde.

Gewohnheiten aufbauen

Handlungen, die nicht automatisiert werden können, müssen den **Mitarbeitern zur Gewohnheit** werden. Dadurch wird verhindert, dass die notwendigen Sicherungsarbeiten immer seltener durchgeführt werden. Der IT-Sicherheitsbeauftragte **überprüft regelmäßig**, dass alle Mitarbeiter sich an die Anweisungen halten. Auch die **Technik** kann helfen: Eine Textmessage oder der Kalender im Smartphone erinnert den Mitarbeiter daran, die Sicherungsarbeiten durchzuführen.

BEISPIEL

Jeden Freitag um 17 Uhr schließt der Mitarbeiter Anton Liebig eine externe Festplatte an den Firmen-PC. Die Datensicherung startet automatisch. Danach übergibt er die Festplatte seinem Chef. Dieser nimmt die externe Festplatte mit nach Hause und bewahrt sie bis Montag früh in einem Stahltresor auf.

Sicherungskopien verschlüsseln

Auch Sicherungskopien müssen vor Diebstahl oder Missbrauch geschützt werden. Der beste Schutz ist die **Verschlüsselung**. Gute Datensicherungsprogramme bieten dies als Option an. Manchmal liegen die Daten bereits in verschlüsselter Form auf dem Rechner und sind daher auf der Sicherungskopie ebenfalls verschlüsselt.

Selbstverständlich müssen alle **Schlüssel** und **Zugangsdaten** (zum Beispiel Passwörter) für die Verschlüsselung auch **gegen Verlust** und **Missbrauch gesichert** werden!

Datensicherung und Dokumentation aktuell halten

Die IT-Technik in einem Unternehmen wird häufig verändert. Daher ist es wichtig, bei jeder Änderung, Erweiterung oder Neuanschaffung zu prüfen, ob die **bestehende Datensicherung überarbeitet** werden muss. Auch die **Dokumentation** muss entsprechend **aktualisiert** werden.

LINKTIPP

Eine umfangreiche Sammlung zum Thema Datensicherung findet sich in der Lehrbuchsammlung von Wikipedia „Wikibooks“:

https://de.wikibooks.org/wiki/Datensicherung

Das Bundesamt für Sicherheit in der Informationstechnik bietet innerhalb seines umfangreichen „IT-Grundschutz“-Programms Beispielprofile für kleine Institutionen und den Mittelstand an. Diese enthalten auch Informationen zur Datensicherung:

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/hilfmi/profile/profile.html

LERNEINHEIT 3: DATENSICHERUNG UND NOTFALLPLANUNG

UNTERRICHTSVERLAUF

4 Schulstunden á 45 Minuten

1. SCHULSTUNDE

Thema	Inhalt und Methode	Arbeitsform	Material	Dauer
Vorbereitung	> Aufbau & Technik-Check			
Einstieg und Begrüßung	> Start mit SuS: Begrüßung und kurze Vorstellung	Plenum		5 Min
Austausch: Daten in Unternehmen	> Diskussion im Plenum: Welche Arten von Daten gibt es im Unternehmen? Welche davon sind „lebenswichtig“? > Brainstorming mit Hilfe einer Web-Anwendung. Beispiele: https://answergarden.ch https://www.mentimeter.com > Alternative: ggfs. Sammlung an Tafel, Whiteboard, Flipchart o.ä. > Vergleich mit PowerPoint Folie Kap. 1: Schutz aller Unternehmensdaten > Diskussion	Plenum	> Smartphones oder Computer mit Internetzugang, Brainstorming-App, Beamer oder Smartboard > Tafel, Whiteboard oder Flipchart, ggfs. Eddings > PC/Laptop mit Beamer/Smartboard, Speichermedium mit PowerPoint Präsentationsfolien LE 3	15 Min
Wissensvermittlung: Lehrfilm „Datensicherung und Notfallplanung“	> 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	20 Min
Abschluss	> Ggfs. offene Fragen klären > Ausblick für die nächste Stunde > Wenn nicht Schulstunde 4 durchgeführt wird: Aushändigung des Transfermaterials (Poster, Checkliste, Arbeitsauftrag) sowie der ausgedruckten PowerPoint Folien als Handout	Plenum	> Ggfs. Transfermaterialien (Poster, Checkliste, Arbeitsauftrag etc.) & Handouts (PowerPoint Folien LE3)	5 Min

2. SCHULSTUNDE

Thema	Inhalt und Methode	Arbeitsform	Material	Dauer
Vorbereitung	> Aufbau & Technik-Check > Evtl. Bildung von Gruppenarbeitstischen			
Einstieg und Begrüßung	> Start mit SuS: Begrüßung und kurze Vorstellung	Plenum		5 Min
Gruppenarbeit: Datenverlust in Unternehmen – Risikofaktoren	> Bildung von Kleingruppen > Pro Gruppe einen Arbeitsbogen AB3a: Datenverlust in Unternehmen – Risikofaktoren > SuS diskutieren Fragen und erstellen eine Liste mit Risikofaktoren > Vergleich mit Internetseite Wikibooks „Datensicherung“ unter: https://de.wikibooks.org/wiki/Datensicherung/_Risiken und/oder PowerPoint Folie (Kap. 2 Gründe für Datenverlust)	Kleingruppen Kleingruppen oder Plenum	> Gruppenarbeitsbögen AB 3a > PC/Laptop > Beamer oder Smartboard > Internetzugang oder ggfs. Speichermedium mit PowerPoint Präsentation LE 3 > Ggfs. Nutzung eigener Smartphones	25 Min
Brainstorming: Datensicherung	> Erste kurze Diskussion darüber, wie Datensicherung erfolgen könnte > Ggfs. Notizen an Tafel o.ä.	Plenum	> Tafel, Whiteboard oder Flipchart > Ggfs. Eddings	10 Min
Abschluss	> Ggfs. offene Fragen klären > Ausblick für die nächste Stunde > Wenn nicht Schulstunde 4 durchgeführt wird: Aushändigung des Transfermaterials (Poster, Checkliste, Arbeitsauftrag) sowie der Folien als Handout	Plenum	> Ggfs. Transfermaterialien (Poster, Checkliste, Arbeitsauftrag etc.) & Handouts (PowerPoint Folien LE3)	5 Min

3. SCHULSTUNDE

Thema	Inhalt und Methode	Arbeitsform	Material	Dauer
Vorbereitung	> Aufbau > Evtl. Bildung von Gruppenarbeitstischen			
Einstieg und Begrüßung	> Start mit SuS: Begrüßung und kurze Vorstellung	Plenum		5 Min
Wissens-Check und Transferübung: Unzureichende Datensicherung	> Bildung von Kleingruppen > Austeilen des Leittextes sowie des Arbeitsauftrags für die SuS AB 3b > Lesen des Textes und Beantwortung der Fragen in der Kleingruppe. > Alternativ: SuS lesen den Leittext in Einzelarbeit und beantworten anschließend die Fragen mit oder ohne den Leittext in Einzelarbeit (Kann auch als LEK genutzt werden) > Diskussion der Ergebnisse im Plenum	Kleingruppen oder Einzelarbeit Plenum	> AB 3b: Unzureichende Datensicherung	35 Min
Abschluss	> Ggfs. offene Fragen klären > Ausblick für die nächste Stunde > Wenn nicht Schulstunde 4 durchgeführt wird: Aushändigung des Transfermaterials (Poster, Checkliste, Arbeitsauftrag) sowie der Folien als Handout	Plenum	> Ggfs. Transfermaterialien (Poster, Checkliste, Arbeitsauftrag etc.) & Handouts	5 Min

4. SCHULSTUNDE

Thema	Inhalt und Methode	Arbeitsform	Material	Dauer
Vorbereitung	> Aufbau & Technik-Check			
Einstieg und Begrüßung	> Start mit SuS: Begrüßung und kurze Vorstellung	Plenum		5 Min
Wiederholung: PowerPoint Präsentation	> Präsentation der PowerPoint Folien (Kap. 3) durch die Lehrkraft: Die Datensicherung > Ggfs. Diskussion im Plenum	Plenum	> PC/Laptop > Beamer oder Smartboard > Speichermedium mit PowerPoint Präsentation LE 3	15 Min
Wissens-Check: Quiz	> Beantwortung des Quiz Q1 durch SuS auf Papier oder online auf der Bottom-Up Webseite unter www.dsin-berufsschulen.de > Alternativ: Bearbeiten der QR-Code-Rallye QR1 (Hinweis: diese Methode dauert etwa 10 - 15 Minuten länger, ggfs. die Diskussion kürzen) > Vergleich und Diskussion der Lösungen	Einzel- oder Gruppenarbeit Plenum Plenum	> Arbeitsbogen Q3 bzw. Smartphone o. Computer mit Internetzugang > ausgedruckte QR-Codes, Arbeitsbogen QR1 und Smartphones mit QR-Code-Scanner	15 Min
Abschluss	> Ggfs. offene Fragen klären > Aushändigung der ausgedruckten PowerPoint Folien als Handout > Aushändigung und kurze Erläuterung des Transfermaterials: Poster, Checkliste & Arbeitsauftrag	Plenum	> Transfermaterialien (Poster, Checkliste, Arbeitsauftrag etc.) > Handouts (PowerPoint Folien LE 3)	10 Min

ARBEITSBOGEN GRUPPENARBEIT AB 3A: DATENVERLUST IN UNTERNEHMEN – RISIKOFAKTOREN

Arbeitsauftrag

1. Bilden Sie Kleingruppen.
2. Diskutieren Sie: Wie können Daten verloren gehen? Welche Risikofaktoren gibt es?
3. Erstellen Sie eine Liste.
4. Vergleichen Sie diese mit der Liste in „Datensicherung“ bei Wikibooks: https://de.wikibooks.org/wiki/Datensicherung/_Risiken
5. Alternative: Vergleich mit PowerPoint Folie Kap. 1: Schutz aller Unternehmensdaten

ARBEITSBOGEN AB 3B: UNZUREICHENDE DATENSICHERUNG

LÖSUNG FÜR DIE LEHRKRAFT

Arbeitsauftrag

Der Leittext kann zum einen als selbstständige Erarbeitung der Inhalte oder als Hilfestellung zur Beantwortung der Fragen dienen.

Bei dem dargestellten Szenario sollen die Schüler*innen mögliche Risiken hinsichtlich der Datensicherung erkennen und hierzu die Fragen entsprechend beantworten. Dies kann in Einzel- oder Gruppenarbeit geschehen.

Diese Aufgabe kann auch als Lernerfolgskontrolle genutzt werden.

Lösung:

1. Laptop, Desktop-PC, Tablet-Computer, Smartphone
2. Smartphone (Daten liegen auch beim Cloud-Dienst und auf dem Laptop)
3. Laptop und Desktop-PC (auf dem Tablet liegen keine unternehmenswichtigen Daten)
4. Angebote und Aufträge sowie E-Mails
5. Finanzbuchhaltung, E-Mails
6. Mögliche Antworten können hier nur skizziert werden:

   Von der 3-2-1-Regel ausgehend:

   > Drei Kopien: Desktop-PC, (externe) Festplatte oder USB-Stick, zweite externe Festplatte oder Cloud-Dienst
   > Zwei unterschiedliche Datenträger: Automatisch erfüllt, wenn zum Desktop-PC ein externer Datenträger (Festplatte, USB-Stick) benutzt wird
   > Eine „offsite“-Kopie: Diese Bedingung ist erfüllt, wenn ein Cloud-Dienst benutzt oder eine zweite externe Festplatte außerhalb des Büros gelagert wird

   Weitere wichtige Aspekte:

   > Wann, wie oft? So oft wie möglich, feste Zeiten, z.B. dreimal am Tag oder jeden Freitag, eine Kalendererinnerung kann helfen
   > Sicherungsprogramm: Startet automatisch die Datensicherungen
   > Regelmäßig (ggfs. mit Verantwortlichen) prüfen, dass die Sicherungskopie lesbar ist
   > Sicherungskopien an einem sicheren Aufbewahrungsort lagern.

ARBEITSBOGEN AB 3B: UNZUREICHENDE DATENSICHERUNG

Arbeitsauftrag

1. Lesen Sie zunächst den Leittext und anschließend das beschriebene Szenario aufmerksam durch.
2. Beantworten Sie dann die untenstehenden Leitfragen.

Leittext

Ziel einer **ausreichenden Datensicherung** ist es, dass **alle wichtigen Daten jederzeit wiederherstellbar** sind. Hat man eine Datei versehentlich gelöscht oder wurde der Computer gestohlen oder zerstört, ist es möglich, alle Daten aus Sicherungskopien auf einen neuen Computer zu kopieren.

IT Sicherheitsbeauftragte benennen

Die Datensicherung muss sorgfältig geplant und durchgeführt werden – und zwar regelmäßig. Dazu gehört, dass es verantwortliche Personen gibt, die im Notfall wissen, was zu tun ist. Herzu benennt das Unternehmen eine*n IT-Sicherheitsbeauftragte*n sowie eine*n **Stellvertreter*in**.

Datensicherung planen

Für eine sorgfältige Planung werden als erstes **alle Daten und Geräte aufgelistet**, die gesichert werden müssen. Wichtig ist, **alles vollständig zu erfassen**. Dann wird für jede dieser Daten und Geräte **festgelegt, wie sie gesichert** werden.

Die 3-2-1-Regel – ein praktisches Mittel hierfür

3: Es werden **drei** Kopien gesichert (die Originaldaten zählen mit).
2: Diese sind auf mindestens **zwei** unterschiedlichen Datenträgern gelagert.
1: Eine Kopie wird extern (offsite – außerhalb des Büros, der Werkstatt usw.) aufbewahrt.

Plan umsetzen

Der fertige Plan wird nun umgesetzt: Datenträger und Software werden angeschafft und installiert. Eine wichtige Aufgabe ist, die **Mitarbeiter*innen ausreichend einzuweisen**. Denn einige Arbeiten sind nicht automatisierbar, zum Beispiel die externe Festplatte an den Computer zu schließen, oder den Datenträger an einen sicheren Ort zu transportieren.

Wichtig: Alles Dokumentieren

Nicht immer ist der bzw. die Verantwortliche für die Datensicherung erreichbar. Daher muss alles in einer **Dokumentation schriftlich festgehalten** werden. Damit können Vertreter*innen, andere Mitarbeiter*innen oder externe Expert*innen nachvollziehen, wie die Datensicherung im Unternehmen funktioniert. Es lohnt sich, die Dokumentation auszudrucken und an einem sicheren Ort aufzubewahren.

Regelmäßig die Sicherheitskopien überprüfen

Wer Daten nur sichert, hat das Wichtigste vergessen: Man muss **regelmäßig überprüfen**, ob die Daten auf den **Sicherungskopien** auch **wiederherstellbar** sind.

Datensicherungen automatisieren

Eine gute Datensicherung lässt **so viel wie möglich automatisch** von dem eingesetzten Datensicherungsprogramm erledigen.

Gewohnheiten aufbauen

Handlungen, die nicht automatisiert werden können, müssen den **Mitarbeiter*innen zur Gewohnheit** werden. Der oder die IT-Sicherheitsbeauftragte **überprüft regelmäßig**, dass alle sich an die Anweisungen halten. Auch die Technik kann helfen: Eine Textmessage oder der Kalender im Smartphone erinnert daran, die Sicherungsarbeiten durchzuführen.

Sicherungskopien verschlüsseln

Auch Sicherungskopien müssen vor Diebstahl oder Missbrauch geschützt werden. Der beste Schutz ist die **Verschlüsselung**. Gute Datensicherungsprogramme bieten dies als Option an. Manchmal liegen die Daten bereits in verschlüsselter Form auf dem Rechner und sind daher auf der Sicherungskopie ebenfalls verschlüsselt. Selbstverständlich müssen alle **Schlüssel** und **Zugangsdaten** (zum Beispiel Passwörter) für die Verschlüsselung auch **gegen Verlust** und **Missbrauch gesichert** werden!

Datensicherung und Dokumentation aktuell halten

Die IT-Technik in einem Unternehmen wird häufig verändert. Daher ist es wichtig, bei jeder Änderung, Erweiterung oder Neuanschaffung zu prüfen, ob die **bestehende Datensicherung überarbeitet** werden muss. Auch die **Dokumentation** muss entsprechend **aktualisiert** werden.

Leitfragen

> Wie viele Geräte gibt es im Betrieb von Antonia Lustig?

> Auf welchen Geräten ist bereits eine Datensicherung vorhanden?

> Auf welchen Geräten muss eine Datensicherung installiert werden?

> Welche Daten des Laptops müssen gesichert werden?

> Welche Daten des Desktop-PCs müssen gesichert werden?

> Skizzieren Sie kurz ein Datensicherungskonzept für den Desktop-PC mithilfe der 3-2-1-Regel.

Das Szenario

Im Handwerksbetrieb von Antonia Lustig gibt es zwei Rechner: Den Laptop der Firmenchefin sowie den Desktop-PC im Büro des Sekretärs Boris Ganz. Auf dem Laptop befinden sich die Angebote und Aufträge. Auf dem Desktop-PC befinden sich die Finanzbuchhaltung und die Personaldatenbank. Beide benutzen E-Mail, um Dokumente auszutauschen. In der Werkstatt gibt es noch einen Tablet-Computer, der nur zum Nachschlagen in Katalogen und Datenbanken im Internet verwendet wird. Auf dem Smartphone empfängt Antonia Lustig E-Mails und Textmessages. Dort gibt es eine Kontaktliste mit Adressen, Telefonnummern und E-Mail-Adressen von Kund*innen und Lieferant*innen. E-Mails, Messages und die Kontaktliste werden über den Cloud-Dienst des Smartphone-Herstellers sowohl mit dem Smartphone als auch mit dem Laptop synchronisiert.

ARBEITSBOGEN: QUIZ Q3

(Mehrfachnennung möglich)

1. Wie wichtig ist eine Datensicherung für ein Unternehmen?

A Nicht besonders wichtig - Unternehmen sind gegen Datenverlust versichert.
B Es reicht aus, wenn Mitarbeiter*innen in einer Freistunde mal Daten sichern.
C Eine Datensicherung ist notwendig für ein Unternehmen; ein Datenverlust ist jederzeit möglich und kann teuer werden.

2. Wie viel kann die Wiederherstellung der Daten einer Festplatte kosten?

A Zehn bis hundert Euro.
B Um die tausend Euro.
C Mehrere hunderte bis mehrere tausende Euro.

3. Was ist das Ziel einer Datensicherung?

A Alle wichtigen Daten sind aus einer Kopie jederzeit wiederherstellbar.
B Es werden möglichst viele Kopien aller Daten auf dem eigenen Computer gemacht.
C Alle Computer werden nachts in einem feuerfesten Tresor sicher aufbewahrt.

4. Was besagt die 3-2-1-Regel?

A Drei Sicherheitskopien auf zwei unterschiedlichen Datenträgern, eine davon „offsite“.
B Drei unterschiedliche Datenträger mit je zwei Sicherungskopien.
C Drei Mitarbeiter*innen legen auf zwei Datenträgern eine Sicherungskopie an.

5. Was heißt es, eine Sicherungskopie regelmäßig zu überprüfen?

A Man überprüft die Lesbarkeit der Kopien auf Geräten außerhalb des Unternehmens.
B Man geht sicher, dass die Sicherungskopie lesbar ist, indem man einige Daten kopiert und prüft.
C Man prüft, ob die externe Festplatte richtig an dem Computer angeschlossen ist.

6. Welcher der folgenden Aspekte ist keine Ursache für einen Datenverlust?

A Bedienfehler der Mitarbeiter*innen, Diebstahl, Wasserschäden.
B Hard- oder Software Fehler oder Schadsoftware wie Viren.
C Eine Sicherungskopie geht verloren.

7. Für welche Art von Unternehmen ist eine regelmäßige Datensicherung zu empfehlen?

A Selbständige.
B Kleinunternehmen (bis ca. 50 Mitarbeiter*innen).
C Nur größere Unternehmen (ab ca. 50 Mitarbeiter*innen).

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

QR-CODE-RALLYE QR3

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.

S

K

C

A

P

U

B

QR-CODE-RALLYE QR3

LÖSUNG FÜR DIE LEHRKRAFT

1. **Wie wichtig ist eine Datensicherung für ein Unternehmen?**

   Eine Datensicherung ist notwendig für ein Unternehmen; ein Datenverlust ist jederzeit möglich und kann teuer werden.

   B

2. **Wie viel kann die Wiederherstellung der Daten einer Festplatte kosten?**

   Mehrere hunderte bis mehrere tausende Euro.

   A

3. **Was ist das Ziel einer Datensicherung?**

   Alle wichtigen Daten sind aus einer Kopie jederzeit wiederherstellbar.

   C

4. **Was besagt die 3-2-1-Regel?**

   Drei Sicherheitskopien auf zwei unterschiedlichen Datenträgern, eine davon „offsite“.

   K

5. **Was heißt es, eine Sicherungskopie regelmäßig zu überprüfen?**

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

   U

6. **Welcher der folgenden Aspekte ist keine Ursache für einen Datenverlust?**

   Eine Sicherungskopie geht verloren.

   P

7. **Für welche Art von Unternehmen ist eine regelmäßige Datensicherung zu empfehlen?**

   Sowohl für größere Unternehmen (ab ca. 50 Mitarbeiter*innen), als auch für Selbständige und Kleinunternehmen (bis ca. 50 Mitarbeiter*innen).

   S

QR-CODE-RALLYE QR3

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. Wie wichtig ist eine Datensicherung für ein Unternehmen?

2. Wie viel kann die Wiederherstellung der Daten einer Festplatte kosten

3. Was ist das Ziel einer Datensicherung?

4. Was besagt die 3-2-1-Regel?

5. Was heißt es, eine Sicherungskopie regelmäßig zu überprüfen?

6. Welcher der folgenden Aspekte ist keine Ursache für einen Datenverlust?

7. Für welche Art von Unternehmen ist eine regelmäßige Datensicherung zu empfehlen?

ARBEITSAUFTRAG LE3: DATENSICHERUNG UND NOTFALLPLANUNG

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 3 „Datensicherung und Notfallplanung“ dialogorientiert und interaktiv mit Vorgesetzten und Kolleg*innen thematisieren.

Beschreibung

Teilen Sie den Arbeitsauftrag zur LE3 *Datensicherung und Notfallplanung* sowie das Anschreiben für den Ausbildungsbetrieb an die Schüler*innen aus. Zur Erfüllung des Arbeitsauftrags benötigen die Schüler*innen zudem folgende Transfermaterialien:

- Quiz aus LE3 (Entweder in Printform austeilen oder per digitalem Zugriff über die Bottom-Up Webseite unter http://t1p.de/f6vo)
- Checkliste zu LE3
- Poster 1 – IT-Sicherheit betrifft jeden! Datensicherung & Notfallplanung

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 LE3: DATENSICHERUNG UND NOTFALLPLANUNG

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** 3 „Datensicherung & Notfallplanung“ durch (Das Quiz ist auf der Bottom-Up Webseite unter http://t1p.de/f6vo 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** 3 „Datensicherung & Notfallplanung“ 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 1** – IT-Sicherheit betrifft jeden! Datensicherung & Notfallplanung im Betrieb – auf und besprechen Sie gemeinsam die vorgestellten Verhaltensempfehlungen (Das Poster erhalten Sie von Ihrer Lehrkraft).

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:
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.