SCHÜLERMAPPE

SELBSTLERNEINHEIT

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:

1. Datenverlust: Ursachen und Folgen — Seite 3

2. Eine Datensicherung im Unternehmen durchführen — Seite 5

3. Maßnahmen für eine gute Datensicherung — Seite 8

Übungseinheit — Seite 10

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

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.

ANREGUNG

Überlegen Sie: 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*).

ANREGUNG

Überlegen Sie: Wie können Daten verloren gehen? Erstellen Sie eine Liste und vergleichen Sie diese mit der Liste in „Datensicherung“ bei Wikibooks.

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

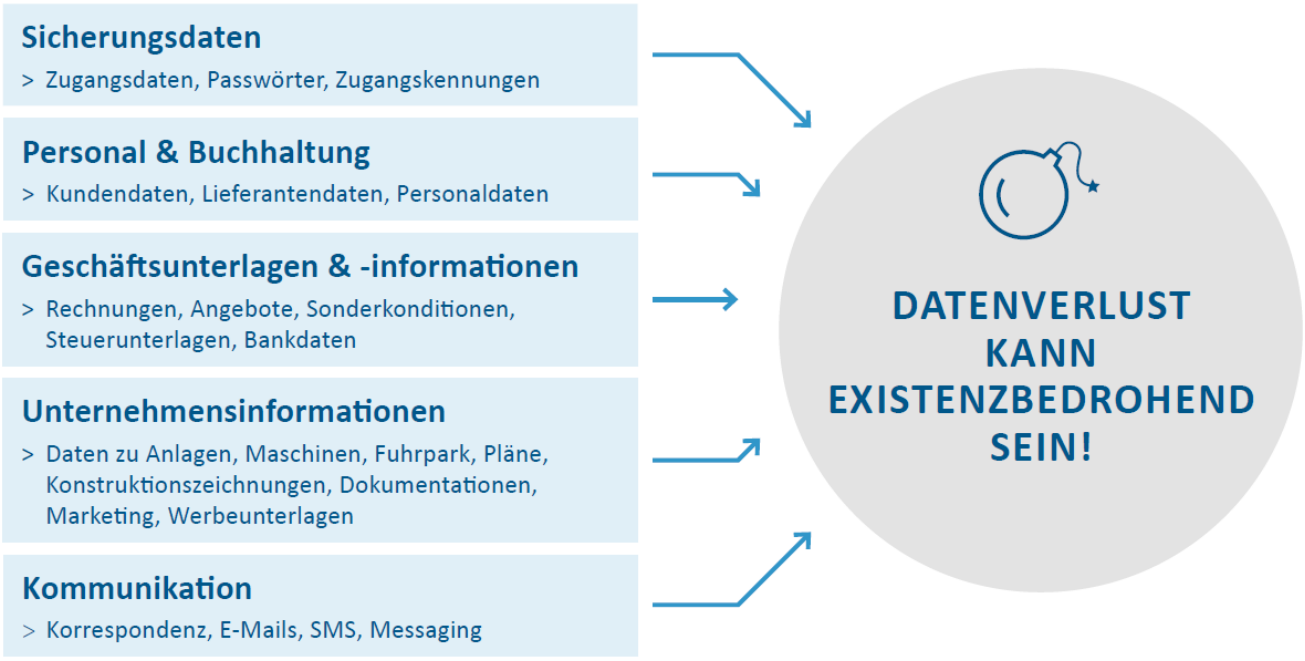
Jeder Datenverlust im Unternehmen kann viel Zeit und Geld kosten. Das Wiederherstellen nur **einer** Festplatte, die nicht gesichert wurde, kann bis zu mehreren **Tausend Euro** kosten – ohne Garantie, dass die Daten wiederherstellt werden können.

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.

ANREGUNG

Fragen Sie in Ihrem Unternehmen nach: 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.

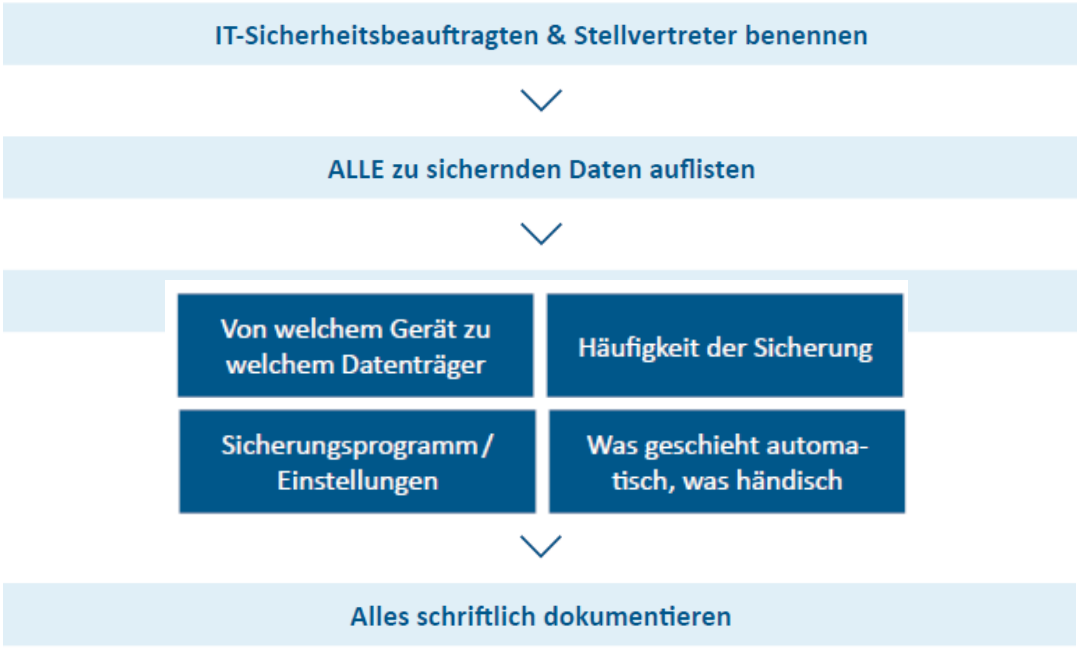
Der fertige Plan wird nun umgesetzt: Datenträger und Software werden angeschafft und installiert. Eine wichtige Aufgabe ist, die **Mitarbeiter ausreichend einzuweisen**. Dies ist ein wichtiger Teil einer Datensicherung. Denn einige Arbeiten sind nicht automatisierbar, zum Beispiel die externe Festplatte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

QUIZ Q3

(Mehrfachnennung möglich)

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

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

1. 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 am 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

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.