



Kapitel 4 - Verantwortungsvoller Umgang mit Daten



In Kooperation mit:



www.zdh.de

In Kooperation mit:



www.bv-ufh.de

Mit freundlicher Unterstützung durch:



www.mmi-hessen.de

Femme digitale – IT-Kompetenz für Frauen im Handwerk

Das ideale Büro - Kompetenzen zur Gestaltung
und Planung der eigenen Büroorganisation

Das Projekt „Femme digitale“ ist Teil der BMWi- Förderinitiative
„Netzwerk Elektronischer Geschäftsverkehr“ (www.ec-net.de)

Darum geht es

Der eigene Arbeitsplatz und das Verhalten des Mitarbeiters stellen häufig die größte Gefahrenquelle für Angriffe auf ein Unternehmen dar.

Im folgenden Kapitel möchten wir Sie darauf hinweisen, welche Gefahren am Arbeitsplatz entstehen können, und wie diese am Besten zu vermeiden sind.

Es werden Gefahren beschrieben, die durch Unwissenheit, Vergesslichkeit oder Bequemlichkeit am Arbeitsplatz auftreten können. Wir möchten Ihnen zeigen, wie Sie diese Gefahren vermeiden und die Sicherheit in Ihrem Unternehmen verbessern können.



Datensicherheit

Für dieses Kapitel
benötigen Sie
ca. 25 Minuten.



Computer-Zugang durch Passwort schützen

Wenn Sie Ihren Arbeitsplatz verlassen, sollten Sie überprüfen, dass Sie Ihren PC ordnungsgemäß gesichert haben.

Die Anlässe in denen Sie Ihren Arbeitsplatz verlassen sind vielfältig: zur Mittagspause, einen Kaffee holen, eine kurze Teambesprechung etc. In diesen Momenten ist Ihr Arbeitsplatz nicht besetzt und Ihr PC ist ein potenzielles Sicherheitsrisiko.

- ▶ Ist Ihr PC auch nur für ein paar Minuten unbeaufsichtigt, müssen Sie sicherstellen, dass niemand auf Ihren Computer zugreifen kann.

Unbeaufsichtigt ist ihr Computer dann, wenn Sie nicht sehen können, was an Ihrem Arbeitsplatz geschieht. Melden Sie sich in diesen Fällen immer korrekt am Computer ab – auch wenn Ihnen dies umständlich erscheint. Nur so können Sie sicher verhindern, dass ein Unbefugter auf vertrauliche Daten zugreifen kann oder Ihr PC zur Gefahrenquelle für Ihr Unternehmen wird.

Sollten Sie nur einen kleinen Botengang erledigen wollen, ist es ausreichend wenn Sie Ihren PC lediglich sperren. Das hat den Vorteil dass die aktuelle Arbeitssitzung erhalten bleibt, der PC aber trotzdem vor neugierigen Blicken und unbefugten Eingaben geschützt ist.



Verhindern Sie, dass Unbefugte Zugriff auf vertrauliche Daten bekommen



Computer-Zugang durch Passwort schützen

Nicht nur beim Verlassen des eigenen Arbeitsplatzes ist das ordnungsgemäße Abmelden am Computer unverzichtbar, sondern auch bei wechselnden Benutzern desselben PCs.

Im Büroalltag kommt es vor, dass verschiedene Benutzer an einem PC arbeiten. Sei es, dass sich zwei Teilzeitarbeitskräfte einen Computerarbeitsplatz teilen oder ein Laptop im Besprechungsraum für jeden Mitarbeiter zur Verfügung steht. Lassen Sie den Einwand, dass ein ordnungsgemäßes An- und Abmelden zu lange dauert, nicht gelten.

Wird bei einem Benutzerwechsel aus Unachtsamkeit oder Bequemlichkeit das ordnungsgemäße An- oder Abmelden vernachlässigt, können Probleme entstehen. Beispielsweise kann nicht mehr nachvollzogen werden, wann welcher Mitarbeiter wie lange an welchem Rechner gearbeitet hat. Ein unter Umständen entlastendes Protokoll zur Beweissicherung kann dann nicht erstellt werden.

Bei einem zentral genutzten PC, an dem sich häufig Benutzer an- und abmelden müssen, kann u. U. ein allgemein gültiges und bekanntes Passwort vergeben werden. Es sollte aber protokolliert werden, was mit diesem PC gemacht wird.



ACHTUNG!

Denken Sie immer daran, sich an Ihrem Computerarbeitsplatz ordnungsgemäß an- und abzumelden.

Daten durch Ordnung schützen

Ein aufgeräumter Arbeitsplatz macht es Angreifern schwer, Daten zu entwenden. Achten Sie stets darauf, dass Sie vertrauliche Daten nie frei zugänglich liegen lassen.

Stapeln sich auf Ihrem Schreibtisch turmhohe Papierstapel, ist das wie eine Einladung für Datendiebe, nach vertraulichen Informationen zu suchen.

Legen Sie deshalb Faxe, Briefe, ausgedruckte E-Mails oder sonstige personenbezogene Daten sofort nach Ihrer Bearbeitung in abschließbaren Schränken ab oder vernichten Sie sie, wenn diese nicht mehr benötigt werden. Sogar Notizzettel können wichtige Informationen enthalten und sollten daher ebenso gegen Missbrauch geschützt werden. Die Gefahr, dass schützenswerte Daten sonst auf einfache Weise ausspioniert werden können ist hoch.

Sichern Sie auch CD-ROMs, DVDs oder USB-Sticks beim Verlassen Ihres Arbeitsplatzes durch Verschlüsselung, denn nicht nur Papier ist eine mögliche Informationsquelle für Angreifer.



Gefährdung von Innen

Sorgen Sie immer dafür, dass vertrauliche Daten unzugänglich für Dritte sind!

Hinweise zur geordneten Datenhaltung

Beim Speichern von Daten auf Datenträgern können verschiedene Probleme auftreten. Vor allem dann, wenn bestimmte Regeln und Richtlinien zur Datenhaltung nicht eingehalten wurden.

Bitte achten Sie darauf, dass Sie Ihre Daten beim Arbeiten strukturiert und sinnvoll ablegen. Dadurch vermeiden Sie z. B. langes Suchen auf Ihrem PC oder im Firmennetzwerk. Achten Sie bitte außerdem darauf, dass Sie Ihre Daten nicht aus Versehen Dritten zugänglich machen, die eigentlich keine Berechtigung besitzen, Ihre Daten zu verwenden. Das geschieht oft dann, wenn Daten im Netzwerk unstrukturiert abgelegt werden.

Vielleicht lohnt sich bei Ihnen ja der Einsatz eines Dokumenten-Management-Systems (DMS), auf dem Markt existieren zahlreiche Softwarelösungen. Prüfen Sie die Möglichkeiten, die Ihnen der Einsatz solcher Systeme bietet.



Suchen und finden...

2,44 Stunden

**benötigt ein Mitarbeiter pro Woche
zum Suchen von Dokumenten!**

3 - 5 % ...

**der Dokumente in einem Unternehmen
verschwinden oder sind unauffindbar!**

Quelle: Steinbeis Transferzentrum

Daten elektronisch archivieren

Je nach Art der Daten müssen diese auf einem geeigneten Medium gespeichert werden.

Bei der Archivierung von Daten sind grundlegende Unterschiede zwischen den verschiedenen Datenträgern wie z. B. Filme oder Wechselmedien wie DVDs zu beachten.

Da solche Datenträger einen immer höheren Stellenwert in der modernen Arbeitswelt einnehmen, sollten Sie wissen, für welchen Zweck Sie welchen Datenträger verwenden. Informieren Sie sich Ihren Aufgaben entsprechend über die Einsatzmöglichkeiten der verschiedenen Archivierungsmittel.

Wie Sie in der Tabelle sehen können, kann es sinnvoll sein, wichtige Daten von Ihrer Festplatte auf einem separaten Datenträger mit längerer Lebensdauer zu sichern.

Unabhängig vom Datenträger, ist natürlich auch das Datenformat zu überprüfen, dies ist insbesondere bei Langzeitarchivierungen zu beachten.

Lebensdauer von Speichermedien

Steintafeln und -malereien	mehrere 1000 Jahre
Säurefreies Papier	mehrere 100 Jahre
Säurehaltiges Papier	70 - 100 Jahre
Herkömmliche Bücher	100 - 200 Jahre
Mikrofilm	ca. 500 Jahre (teilw. < 50 Jahre)
Filme auf Zelluloid	mehrere 100 Jahre (oft nur 50 - 70 Jahre)
CD-ROM und DVD-ROM	25 - 100 Jahre
CD-R/-RW und DVD-R/-RW	z. T. < 5 Jahre
Zeitungspapier	10 - 50 Jahre
Disketten	5 - 10 Jahre
Magnetbänder	Bis zu 30 Jahre (teilw. < 10 Jahre)
USB-Stick	3 - 10 Jahre
Festplatte	ca. 10 Jahre

Daten elektronisch archivieren

Wenn die Archivierung von Datenbeständen zu Ihren Aufgaben gehört, müssen Sie unter allen Umständen auf die aktuelle Rechtsprechung achten.

Halten Sie Gesetze zur Archivierung bestimmter Unternehmensunterlagen nicht ein, kann dies straf- und zivilrechtliche Folgen haben. Sie fügen damit nicht nur Ihrem Unternehmen Schaden zu, sondern riskieren auch Ihren Arbeitsplatz zu verlieren, wenn Sie Daten nicht ordnungsgemäß archivieren. Sie müssen Daten immer in einer Form archivieren, die uneingeschränkte Kontrollen durch zuständige Behörden ermöglicht. Bestimmte Daten müssen

- ▶ Unverfälscht,
- ▶ für Dritte verstehbar und
- ▶ ohne Verzögerung einsehbar sein,

Falls Sie sich in Detailfragen nicht sicher sein sollten, kann eine Rechtsberatung nicht schaden.



Eine Liste der zur Zeit geltenden Aufbewahrungsfristen finden Sie bei den Servicefunktionen unter LINKS

Dort finden Sie unter Anderem die Fristen für die Aufbewahrung von Datenträgern, Buchungsbelegen, Arbeitsanweisungen etc.



Daten elektronisch archivieren

Datenträger sollten für den Postweg besonders stabil und sicher verpackt werden.

Wenn Sie Daten auf dem Postweg versenden, ist es wichtig, dass die Verpackung so gestaltet ist, dass der Inhalt auch bei Beschädigung der Hülle nicht verloren gehen kann. Wählen Sie daher immer eine Verpackung, die diesen Kriterien entspricht. Kleine Datenträger sollten Sie immer so verpacken, dass sie nicht aus Versehen entsorgt werden, weil das Päckchen den Anschein erweckt, außer dem Anschreiben nichts zu enthalten.

Der häufigste Grund für falsche oder nicht zugestellte Lieferungen ist eine fehlerhafte Postadresse. Oberste Priorität beim Versand wichtiger Daten hat deshalb die korrekte Anschrift. Bitte vermerken Sie auch, ob der Empfänger das Päckchen nur persönlich in Empfang nehmen darf. Sind Daten oder Datenträger besonders wertvoll, sollte das Paket versichert und gegebenenfalls ein spezieller Dienstleister gewählt werden.

Datenträger sollten nur verschlüsselt weitergegeben werden. Das gilt vorallem für Wechseldatenträger wie CDs oder USB-Sticks, aber auch für Festplatten in Laptops oder PDAs. Nur so können Sie sichergehen, dass bei Verlust des entsprechenden Datenträgers, keine negativen Folgeschäden zu erwarten sind.



HINWEIS:

Verwenden Sie nur geeignete Versandtaschen, um Verluste auf dem Postweg zu vermeiden.

Daten elektronisch archivieren

Sie sollten Datenträger so kennzeichnen, dass sofort der Inhalt, der Bearbeitungsstand und die verantwortliche Person zu erkennen ist.

Für Ihre eigenen Arbeitsunterlagen mag es unerheblich sein in welcher Art Sie Datenträger kennzeichnen. Aber sobald Ihre Kollegen oder externe Mitarbeiter darauf zugreifen müssen, ist eine korrekte Kennzeichnung unverzichtbar. Sobald die Zahl der ausschließlich von Ihnen verwendeten Datenträger einen gewissen Umgang überschreitet, sollten diese ebenfalls aussagekräftig beschriftet werden.

Wenn Sie mehrere Datenträger an eine Person versenden, kann es bei nicht ausreichender Beschriftung zu Verwechslungen der Medien kommen. Bitte beschriften Sie Datenträger sorgfältig. Versehen Sie auch gebrannte CDs und DVDs mit aussagekräftigen Angaben. Das verkürzt das Suchen und hilft den versehentlichen Verlust von Daten zu vermeiden.



**Durch eine aussagekräftige
Beschriftung von Datenträgern
können Suchzeiten minimiert
werden ...**



Datenschutz beim Datenaustausch

Wenn Sie Daten versenden, sollten Sie darauf achten, dass Sie nur die Datensätze auswählen, die auch für den Versand bestimmt sind.

Gelegentlich kommt es vor, dass Sie nicht nur einzelne Dateien versenden möchten, sondern evtl. ganze Verzeichnisse. Prüfen Sie zuvor, dass in diesen Verzeichnissen nur die Dateien enthalten sind, die versandt werden sollen. Entfernen Sie Dokumente mit veralteten Arbeits- oder Planungsschritten, die der Empfänger nicht sehen soll oder darf.

Kontrollieren Sie vor dem Versand von E-Mails mit Datei-Anhang genau, welche Dateien Sie versenden. Andernfalls können mit wenigen schnellen Mausklicks Daten versendet werden, die nicht für den Empfänger bestimmt waren. Achten Sie bitte auch darauf, dass Sie beim E-Mail-Versand an mehrere Empfänger immer eine aktuelle Verteilerliste benutzen, damit niemand E-Mails erhält, für die er nicht oder nicht mehr die nötige Autorisierung besitzt.

Aus datenschutzrechtlichen Gründen sollten Sie beim Versand von Massen E-Mails darauf achten, alle zusätzlichen Empfänger in das Bcc-Feld (blind carbon copy) einzutragen. So verhindern Sie die unfreiwillige und oft unerwünschte Weitergabe von E-Mail Adressen.



Prüfen Sie nicht nur den Text Ihrer E-Mail sondern auch die Anlage ...

Tipps zum Umgang mit vertraulichen Daten

Vertrauliche Daten müssen mit besonderer Sorgfalt bearbeitet werden.

Wenn Sie mit brisanten Daten arbeiten, müssen Sie in Ihrem Arbeitsalltag auf folgende Dinge besonders achten:

- ▶ Sie sollten niemals personenbezogene Informationen frei zugänglich liegen lassen. Dies gilt insbesondere für Ihren Arbeitsplatz, für Besprechungsräume oder Drucker
- ▶ Bevor Sie Daten mittels Datenträger versenden, müssen Sie prüfen, ob sich Informationen darauf befinden, die nicht für den Empfänger bestimmt sind
- ▶ Daten, die im Internet veröffentlicht werden sollen, müssen hinsichtlich Ihrer Freigabe überprüft werden
- ▶ Zu weit gehende Zugriffsrechte für Mitarbeiter können zum Integritätsverlust führen, wenn unberechtigte Personen Änderungen an Daten vornehmen können

Denken Sie daran bei der Entsorgung von Speichermedien wie z. B. Festplatten daran, alle darauf gespeicherten Daten zu vernichten, und zwar so, dass sie nicht wieder hergestellt werden können (z. B. physisch zerstören).



Sie kennen ja das Sprichwort:
„Vertrauen ist gut, Kontrolle ist besser“, gerade bei vertraulichen Daten sollten Sie genau hinschauen



Datenschutzbeauftragter

Unter Umständen kann es erforderlich sein, dass Sie gesetzlich dazu verpflichtet sind, einen Datenschutzbeauftragten für Ihren Betrieb zu benennen.

Das ist dann der Fall, wenn einer der folgenden vier Punkte auf Ihren Betrieb zu trifft:

- ▶ wenn personenbezogene Daten elektronisch (mit Hilfe der EDV) erhoben, verarbeitet oder genutzt werden und damit 9 oder mehr Arbeitnehmer ständig beschäftigt sind.
- ▶ wenn personenbezogene Daten auf andere Weise (ohne die EDV) verarbeitet werden und damit 20 Arbeitnehmer oder mehr beschäftigt sind.
- ▶ wenn automatisierte Verarbeitungen vorgenommen werden, die einer Vorabkontrolle gemäß §4d Abs. 5 Bundesdatenschutzgesetz (BDSG) unterliegen (unabhängig von der Anzahl der Arbeitnehmer).
- ▶ wenn personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung verarbeitet oder genutzt werden.

Wenn Sie überprüfen möchten ob Sie in Ihrem Betrieb einen Datenschutzbeauftragten benötigen, können Sie dies schnell mit Hilfe dieses **Selbsttests** ermitteln.



Download

Mehr über das Thema Datenschutzbeauftragter erfahren Sie in diesem Informationsblatt des Bundesbeauftragten für den Datenschutz und Informationssicherheit.



Zusammenfassung

In dem Kapitel „Datensicherheit“ haben Sie erfahren,

- ▶ dass Sie Ihren Arbeitsplatz für unbefugten Zugriff schützen sollten und wie Sie das am einfachsten bewerkstelligen
- ▶ dass eine strukturierte Ablage von Daten nicht nur Zeit spart, sondern auch vor Datenmissbrauch schützt
- ▶ auf was Sie beim elektronischen Archivieren von Daten achten sollten
- ▶ dass Sie beim versenden von E-Mails auch die Anhänge kontrollieren sollten, damit Sie Unbefugten keine vertraulichen Daten zusenden
- ▶ welche Aufbewahrungsfristen bei der elektronischen Archivierung eingehalten werden sollten und welche Datenträger dafür geeignet sind



Zusammenfassung





Diese CD-ROM und PDF ist ein Projekt der BMWi-Förderinitiative „Netzwerk Elektronischer Geschäftsverkehr“.

Netzwerkpartner:



KLICK Rheinland-Pfalz
Bahnhofstraße 30 - 32
54292 Trier
Telefon: 0651 - 9 75 67 0
Telefax: 0651 - 9 75 67 33
Internet: www.klick-net.de
E-Mail: info@klick-net.de



KEGO Oderland
Bahnhofstraße 12
15230 Frankfurt (Oder)
Telefon: 0335 - 56 19 122
Telefax: 0335 - 56 19 121
Internet: www.kego.de
E-Mail: info@kego.de



mdc-ecomm
Dresdner Straße 11/13
04103 Leipzig
Telefon: 0341 - 2 18 82 38
Telefax: 0341 - 2 18 82 49
Internet: www.mdc-ecomm.de
E-Mail: mueller.pnm@hwk-leipzig.de



Externe Netzwerkpartner:

ECCN GbR
Ludwig-Erhard-Str. 4
34131 Kassel
Telefon: 0561 - 3 16 35 90
Telefax: 0561 - 3 16 35 91
Internet: www.eccn.de
E-Mail: info@eccn.de

(CD-ROM Konzept u. Umsetzung)



HBZ Münster - Zentrum IT
und Medientechnologie
Eichelmeyerstraße 1-2
48163 Münster
Telefon: 0251 - 7 05 14 20
Telefax: 0251 - 7 05 14 28
Internet: www.hwk-muenster.de
E-Mail: info@hwk-muenster.de



In Kooperation mit:

Zentralverband des Deutschen
Handwerks
Mohrenstraße 20 - 21
10117 Berlin
Internet: www.zdh.de
E-Mail: info@zdh.de



Bundesverband der Unter-
nehmerfrauen im Handwerk
Mohrenstraße 20 - 21
10117 Berlin
Internet: www.bv-ufh.de
E-Mail: bv-ufh.geschaeftsstelle@zdh.de



Mit freundlicher Unterstützung durch das:

Hessische Ministerium für
Wirtschaft, Verkehr und
Landesentwicklung
Geschäftsstelle hessen-media
Abraham-Lincoln-Straße 38 - 42
65185 Wiesbaden
Internet: www.hessen-media.de
E-Mail: info@hessen-media.de



Gefördert durch das:

Bundesministerium für Wirtschaft
und Technologie (BMWi)
Referat IT-Anwendungen,
Digitale Integration
MinR Dr. Rolf Hochreiter
11019 Berlin
Internet: www.bmwi.de

Haftungsausschluss

In keinem Fall können die im Impressum genannten Unternehmen/ Institutionen oder deren Lieferanten haftbar gemacht werden für direkte oder indirekte Schäden, Folgeschäden oder sonstige Schäden, die aus dem Nutzungsausfall, Verlust von Daten oder entgangenem Gewinn resultieren. Dies gilt für die Verwendung von Software, Dokumenten oder auch Informationen, die auf diesem PDF enthalten sind.

Copyright

Der Inhalt dieses PDFs einschließlich aller seiner Teile ist urheberrechtlich geschützt. Eine Vervielfältigung des Inhaltes oder seiner Teile ist zu kostenlosen Informationszwecken gestattet. Der Inhalt des PDFs darf nicht bearbeitet, ergänzt oder verändert werden. Wird der Inhalt oder Teile davon vervielfältigt, müssen die im Impressum genannten Unternehmen/ Institutionen als Herausgeber aufgeführt werden. Jede Verwertung außerhalb der Grenzen des Urheberrechts- gesetzes ist ohne Zustimmung der Herausgeber unzulässig und strafbar.