DSB+CPD.CH

DER SICHERE UMGANG MIT INFORMATIONS- UND KOMMUNIKATIONSGERÄTEN

Einleitung 2
Schutz gegen Zugriff Unberechtigter 3
- Passwort 3
- Verlassen des Arbeitsplatzes 3
- Löschen, Weitergeben und Speichern von Daten 4

Schutz vor Zerstörung 5
- Viren 5

Kommunikation 6
- E-Mail 6

Netzwerke 7
Tragbare Arbeitsgeräte 8

Die Schweizerischen Daentschutzbeauftragten
www.dsb-cpd.ch

JUNI 2002

Kurz und bündig

Diese Broschüre unterstützt Sie darin, die Hilfsmittel der modernen Informations- und Kommunikationstechnologie optimal zu nutzen und mögliche Gefahren und Risiken zu vermeiden. Sie zeigt Ihnen, wie Sie Ihre Verantwortung für Datenschutz und Datensicherheit wahrnehmen können.

Datenschutz und Datensicherheit. Warum?

Weil nur damit der Schutz der Persönlichkeit gewahrt werden kann – sowohl bei Ihnen als Mitarbeiterin und Mitarbeiter, aber auch bei all denjenigen Personen, deren Daten Sie bearbeiten.

Dieses Thema geht alle an

Wir alle müssen und können unseren Teil an der Verantwortung für Datenschutz und Datensicherheit tragen. In bestimmten Bereichen können nur Sie verhindern, dass Schäden entstehen oder Persönlichkeitsrechte verletzt werden.

Die Verantwortung für Datenschutz und Datensicherheit tragen wir alle!

Passwort

Zweck eines Passwortes

Passwörter sollen sicherstellen, dass nur Berechtigte Zugriff auf ein System oder bestimmte Anwendungen und deren Daten haben. Ansonsten besteht die Gefahr, dass Daten von Unberechtigten eingesehen, manipuliert oder gelöscht werden.

Ein gutes oder starkes Passwort

- Besteht aus mindestens 6, besser 8 oder mehr Zeichen.
- Ist aus Zahlen, Buchstaben und Sonderzeichen kombiniert
- Schreibt sich aus Gross- und Kleinbuchstaben.
- Können Sie sich gut merken, andere aber nur schwer erraten, z.B. Sonn**EN00schein, fRan?ziska57.
- Besteht nicht nur aus Wörtern und Namen, wie sie in einem Wörterbuch oder Lexikon zu finden sind und nicht nur aus Zahlen wie z.B. Telefonnummern, Geburtsdaten oder Auto-Kennzeichen, da diese leicht erraten werden können.

Handhabung des Passwortes

- Halten Sie Ihr Passwort auf alle Fälle **geheim**!
- Ändern Sie das Passwort periodisch, bei Verdacht auf Missbrauch sofort und melden Sie diesen Ihrer vorgesetzten Stelle!
- Verwenden Sie nie exakt dasselbe Passwort für verschiedene Anwendungen!

Verlassen des Arbeitsplatzes

Bei kurzer Abwesenheit

- Sollte stets ein Bildschirmschoner mit Passwortschutz aktiviert sein.
- Dürfen vertrauliche Daten (Papiere, Dossiers, Datenträger) für andere nicht zugänglich sein.

Nach Feierabend

- Ist der Computer vom Netzwerk abzumelden und auszuschalten.
- Sind alle vertraulichen Daten wegzuschliessen.

Bei Ferienabwesenheit

- Sollten Sie Ihre eingehenden Mails nicht automatisch an eine andere Adresse weiterleiten.
- Sollten Sie den Dienst Ihres Mailprogrammes nutzen, mit welchem Sie die Absenderinnen und Absender von E-Mails über Ihre Ferienabwesenheit und Ihre Stellvertretung unterrichten. So können diese selber entscheiden, obsie das E-Mail auch an Ihre Stellvertretung schicken will oder nicht.

Und denken Sie auch daran

- Von Ihnen erkannte Mängel oder Sicherheitslücken müssen behoben werden. Melden Sie diese Ihren Vorgesetzten!
- Auch Wasser und Feuer sind heute noch Gefahrenquellen. Beachten Sie die hierzu notwendigen Vorsichtsmassnahmen!

Löschen, Weitergeben und Speichern von Daten

Löschen von Daten

- Mit Befehlen wie «delete», «erase», «löschen» oder «(Quick)Format» vernichten Sie Daten nicht definitiv, diese bleiben rekonstruierbar. Erkundigen Sie sich bei Ihren Systemverantwortlichen, wie Daten in Ihrem Betrieb unwiederherstellbar gelöscht werden müssen.
- Denken Sie daran, dass Daten oft an unterschiedlichen Orten vorhanden sind. Nicht nur die elektronisch gespeicherten, sondern auch die Daten in Papierform sind zu löschen bzw. zu vernichten.
- Löschen Sie die Daten, bevor Sie ein Gerät weitergeben.

Weitergeben von Daten

- Verwenden Sie zur Weitergabe von Daten wenn immer möglich neue Datenträger, z.B. Disketten.
- Falls Sie gebrauchte Disketten verwenden, formatieren Sie diese zuvor vollständig (Tiefformatierung).

Speichern von Daten

- Schauen Sie darauf, dass vertrauliche Daten stets am richtigen Ort und in verschlüsselter Form abgespeichert werden, so dass nur Berechtigte Zugriff darauf haben , z.B. auf zugangsbeschränkten Ordnern oder auf Disketten.
- Speichern Sie keine Daten auf lokalen Arbeitsplätzen, die nicht gesichert werden.

Viren

Was sind Viren?

Viren, Würmer, trojanische Pferde oder dergleichen sind kleine Programme, die Computersysteme befallen und Daten und Programme zerstören oder verändern oder andere gravierende Schäden anrichten können.

Wie können Viren eingeschleppt werden?

Über E-Mails und Anhänge (Attachments, Dokumente), über Dateien (z.B. Spiele, Freeware), die vom Internet heruntergeladen werden, aber auch über Disketten und CDs. Beachten Sie deshalb die Tipps für einen richtigen Umgang mit E-Mails.

Sie schützen sich vor Viren, indem Sie

- An jedem Arbeitsplatz ein Virenschutzprogramm installieren.
- Virenschutzprogramme nie deaktivieren.
- Disketten und CDs vor dem Gebrauch immer mit dem Virenschutzprogramm prüfen.
- Nur von den Systemverantwortlichen zur Verfügung gestellte, rechtmässig lizenzierte Software verwenden.

Vorgehen bei Auftreten von Viren

- Computer ausschalten.
- Informatik- oder Systemverantwortliche informieren.
- Vorgesetzte informieren.

Vorsicht bei sogenannten «aktiven Inhalten»!

Noch gefährlicher als die Viren sind die sogenannten "aktiven Inhalte", in der Fachsprache oft auch ActiveX-Controls, Java-Applets oder Scripting-Programme genannt, die beim Surfen auf Ihren PC gelangen können. Diese interaktiven Elemente können an Software und Daten grossen Schaden anrichten. Das Sicherheitsrisiko kann mit der richtigen Einstellung Ihres Internetprogrammes (Browsers) verhindert werden. Erkundigen Sie sich bei Ihren Vorgesetzten nach der richtigen Browser-Einstellung.

E-Mail

Risiken und Gefahren

E-Mails können

- an die falsche Adresse gelangen.
- verloren gehen.
- von Unberechtigen gelesen oder manipuliert werden.
- Träger von Viren sein.
- einen vorgetäuschten Absender haben.

Richtiger Umgang mit E-Mail

- Vertrauliche Personendaten und vertrauliche Informationen nur verschlüsselt übermitteln.
- Bei wichtigen E-Mails Empfangsbestätigung anfordern.
- Vergewissern Sie sich, dass Sie das Mail an die richtige Adresse schicken, auch bei Weiterleitung oder Kopie-Zustellung.
- Was für E-Mails gilt, gilt auch für die angehängten Dateien (Attachments)!
- Öffnen Sie nie ein Attachment, das Sie von einem nicht vertrauenswürdigen Person oder Institution erhalten haben.

Internet

Das Internet ist ein offenes Netzwerk. Alle darin publizierten Informationen sind für alle Beteiligten weltweit sichtbar. Einfache Vorsichtsmassnahmen ermöglichen ein sicheres Surfen:

- Schliessen Sie alle anderen Applikationen, während Sie surfen.
- Geben Sie Ihre persönlichen Daten nur an einen vertrauenswürdigen Empfänger, wenn es absolut unumgänglich ist.
- Übermitteln Sie vertrauliche Angaben ausschliesslich verschlüsselt.
- Speichern sie keine vertraulichen Dokumente auf der Festplatte, während Sie online sind.

Intranet

Das Intranet ist ein Netzwerk für einen bestimmten Personenkreis. Ohne zusätzliche Massnahmen im Netzwerkbereich sind grundsätzlich dieselben Vorsichtsmassnahmen wie beim Internet zu treffen. Erkundigen Sie sich bei Ihren Vorgesetzten, welche Sicherheitsregeln Sie beim Gebrauch des Intranets beachten müssen.

Datenspuren

Wer surft, hinterlässt Spuren auf der Arbeitsstation (Cookies, Cache, Verlauf, AutoVervollständigen) und auf dem Server (Protokollierungen).

- Ein Cookie ist eine kurzes Textfile, das auf Ihrer Arbeitsstation gespeichert wird. Ein Anbieter kann mit Hilfe dieser Cookies herausfinden, wann Sie zum letzen Mal auf seiner Site waren und welche Angebote Sie interessierten.
- Im Cache sind die von Ihnen besuchten Internetsites abgespeichert. Dies erlaubt es, die Sites schneller wieder zu laden.
- Auf Ihrer Arbeitsstation werden auch im Verlauf (History) Angaben zu den besuchten Sites gespeichert, damit Sie diese leichter wieder finden.
- Die Funktion des AutoVervollständigen speichert Ihre früheren Eingaben und schlägt diese wieder vor, wenn Sie dasselbe neu eingeben.

Löschen Sie Cookies, Cache, Verlauf und AutoVervollständigen regelmässig!

- Die Protokollierungen enthalten Informationen über alle Aktivitäten, die Sie auf Ihrer Arbeitsstation ausgeführt haben. Diese Angaben werden auf dem Server gespeichert und enthalten unter anderem Ihre IP-Adresse, den Zeitpunkt und die besuchten Sites. Als Anwenderin/Anwender haben Sie keine Möglichkeit, diese Angaben zu löschen.
  Die Datenspuren zeigen auch die private Nutzung von Informatikmitteln auf. Klären Sie ab, ob und unter welchen Bedingungen Ihnen die private Nutzung von Informatikmitteln erlaubt ist.
- Welche Datenspuren auf Ihrem Arbeitsgerät festgehalten und gespeichert werden, können Sie (mindestens teilweise) selbst bestimmen. Orientieren Sie sich bei Ihrer Informatik-stelle nach den Einstellungs- und Löschmöglichkeit auf Ihrer Arbeitsstation.

Mobil Arbeiten

Laptops, Personal Digital Assistants (PDAs) oder Mobiltelefone müssen besonders geschützt werden, da sie nicht nur im eigenen Büro verwendet werden, sondern auch in der Öffentlichkeit.

Verschlüsselung

Jeder Laptop sollte mit einem Verschlüsselungsprogramm ausgerüstet sein. So ist es möglich, einzelne Dateien, bestimmte Bereiche oder die ganze Festplatte so zu verschlüsseln, dass nur Berechtigte Zugang zu den Daten haben.

Diebstahl

- Die Gefahr eines Diebstahls ist bei tragbaren Geräten besonders gross.
- Der Zugang zu den Daten sollte mindestens mit einem Passwort geschützt werden.
- Der Passwortschutz soll zusammen mit dem Bildschirmschoner bereits nach wenigen Minuten einsetzen.

Gemeinsam genutzte Geräte

- Löschen Sie alle vertraulichen Daten, bevor Sie den Laptop weitergeben.
- Speichern Sie Ihre Daten auf einer Diskette. Dies schützt zusätzlich vor Verlust.
- Hinterlassen Sie keine nicht-arbeitsrelevanten Daten.

Vertrauliches an der Öffentlichkeit

Wer zum Beispiel im Zug mit mobilen Arbeitsgeräten arbeitet, muss daran denken, dass Unbeteiligte auf den Bildschirm des Laptops sehen und die Gespräche auft dem Mobiltelefon mithören können.

Spuren löschen

- Löschen Sie vor der Rück- oder Weitergabe des Laptops die Cookies, das Cache, den Verlauf und das AutoVervollständigen.
- Leeren Sie auch den Papierkorb.

Diese Regeln gelten sinngemäss auch für andere mobile Arbeitsgeräte wie z.B. Mobiltelefone oder Handhelds.