Datensicherheit

- kein Buch mit 7 Siegeln!

Heutzutage gibt es wohl keinen aktiv am Geschäftsleben teilnehmenden Nutzer von Computertechnik mehr, der sich nicht schon mal Sorgen um abhanden gekommene Daten gemacht hat.

INFORMATIONS TECHNIK Fachbetrieb

Solange es sich im privaten Bereich nur um leicht wieder beschaffbare Musiktitel oder Filmchen handelt, ist das alles kein Problem. Wer aber im schöpferischen Bereich plötzlich einen seitenlangen, durchgestylten Text nicht wiederfindet, oder aber die gesamten Dokumentationsfotos einer Begutachtung vermisst, kommt schon mal ins schwitzen.

Was aber ist, wenn die Kunden- oder Lieferantendatei versehentlich gelöscht wurde? Welcher Arbeitsaufwand ist damit verbunden die Buchhaltung zu rekonstruieren, wenn die letzte Datensicherung nicht auf dem Laufenden war?

Wie peinlich ist es, wenn persönliche Daten abhanden gekommen sind und in fremden Händen missbraucht werden könnten?

Bundesdatenschutzgesetz (BDSG). In allen Fällen müssen gesetzliche Vorgaben gemäß dem Bundesdatenschutzgesetz mit seinen letzten Änderungen vom 1.4.2010 eingehalten werden. Hiernach gilt es diverse sicherheitsrelevante Daten geheim zu halten und dafür zu sogen, dass gesetzliche und betriebliche Grundlagen zur Datensicherheit strikt eingehalten werden.

Dazu gehört auch, dass die komplette EDV-Hardware gegen Diebstahl gesichert werden muss, aber auch das kriminelle Kopieren von Dateien auf irgendwelche Datenträger. Selbst wenn nichts aus der EDV heraus kopiert wird, sondern fremde Software oder fremde Daten eingespielt werden, ist die Gefahr des Verlustes von Daten recht hoch, denn Schadprogramme werden oft unbemerkt installiert und zerstören im Hintergrund - ggf. zunächst unbemerkt - die angelegten Dateistrukturen.

Die meisten Rechner sind heute über Netzwerke ins Internet eingebunden und per E-Mail zu erreichen, sodass auch hier die Gefahr besteht sich Schadprogramme einzufangen, oder aber dass eigene, ungeschützte Daten unterwegs abgefangen und missbraucht werden. Wer hier nicht auf tagesaktuelle „Schädlingsbekämpfungs-Software“ setzt, hat es schnell mit Viren, Trojanern und Würmern zu tun, die die Arbeit vieler Stunden zunichte machen können.

Daher ist es besonders wichtig bestimmte Regeln einzuhalten:

Passwort-Richtlinien!

Achten Sie darauf, dass verbindlich eingeführte Regeln zur Nutzung und regelmäßigen Änderung von Passwörtern eingehalten werden. Sollte mal ein portables Gerät in die falschen Hände geraten, verhindert ein geschützter Zugang, dass Unberechtigte auf die Daten zugreifen können.

Verschlüsselung von E-Mails!

Schützen Sie sicherheitsrelevante Daten, die per Mail von oder zu einem mobilen Gerät verschickt werden, mit einem hochwertigen Verschlüsselungs-Algorhithmus. Wer es zunächst mit einer kostenlosen Software versuchen will, wird auf den „Freeware-Portalen“ im Internet leicht fündig.

USB-Schnittstelle, CD-ROM, DVD, Disketten-Laufwerk …

Fast alle Geräte verfügen über diese typischen, meistens leicht zugänglichen Schnittstellen, über die ggf. Schad-Programme in den Rechner hinein-, oder auch sensible Daten heraus transportiert werden können. Diese Zugänge können mit geeigneten Mitteln, sowohl mechanisch, als auch elektronisch gesperrt werden.

Wechselmedien wie USB-Sticks, oder die sehr beliebten, großvolumigen USB-Festplatten sowie Pocket-PC, Blackberrys oder Fotohandys können potenzielle Träger von Problemdaten sein und nutzen meistens die USB-Schnittstellen der PC´s, aber auch IR- und Bluetooth Ad hoc-Pico-Netzwerke in der nächsten Umgebung.

Bluetooth-Datenübertragung

Wer ahnt schon, dass die per Bluetooth übertragenen Daten meistens weiter reichen als man denkt. Man sollte daher mobile Geräte für diese Art der Datenübertragung möglichst sperren, sofern man nicht genau weiß, in welcher Umgebung man was überträgt. Wenn hier auch noch die Standard-Passwörter verwendet werden, haben Datenräuber leichtes Spiel.

Datensicherheit durch Fernwartung

Viele Praktiker kennen die Vorzüge der Fernwartung. Ob ein up date an der TK-Anlage vorgenommen werden soll, oder die Warenwirtschaft neu konfiguriert oder auch nur damit gearbeitet werden soll - per Fernwartung ist dieses komfortabel möglich. Hat man so ein nützliches Tool z.B. auf einem Notebook, so könnte man damit im Falle des Diebstahls und der Wiederinbetriebnahme sowie dem Einloggen ins Internet an einem beliebigen Ort per Fernwartung eine (hoffentlich noch rechtzeitige) Datenlöschung auf dem Gerät vornehmen., so dass der Dieb nur noch einen leeren Festplattenspeicher vorfindet.

Entsorgung und Verkauf von EDV-Komponenten

Da nicht nur im Informationstechniker-Handwerk mit sensiblen, ggf. gesetzlich geschützten Daten gearbeitet wird, muss mit z.B. alten Festplatten und sonstigen Speichern sehr sorgfältig umgegangen werden. Hier ist sicher zu stellen, dass auch wirklich alle Daten mit einem geeigneten Programm oder aber durch mechanische Zerstörung gelöscht worden sind. Auch der Weiterverkauf von z.B. in Zahlung genommenen Geräten ist kritisch zu betrachten, da auch hier ggf. Restdaten vorhanden sein könnten, die zur Wiederherstellung ganzer Dateisysteme ausreichen könnten. Es muss also die vollständige und endgültige Löschung von Informationen sichergestellt sein.

Nutzungsregeln für private Geräteim Unternehmen.

Sicherheits-Richtlinien sollten eine Selbstverständlichkeit sein - jeder Mitarbeiter sollte z.B. wissen, dass MP-3 Player und Handys nicht an die Infrastruktur des Unternehmens angeschlossen gehören.

Mitarbeiterschulung

Alle Mitarbeiter sollten wissen, wieso in einem Unternehmen so gehandelt werden muss, wie es zuvor beschrieben wurde. Nur dann, wenn jeder für die Problematik der Datensicherheit sensibilisiert wurde, kann man darauf hoffen, dass ein umfassender Schutz gewährleistet ist und sich der Unternehmer oder auch die Mitarbeiter nicht strafbar machen.

Hochwertige Sicherheitssoftware

Ob Back Up-Software, RAID-Systeme, die Einhaltung verschiedener Back-Up Level, Tages-, Wochen-, Monatssicherungen usw. – immer geht es nur darum, dass im Falle eines Falles alles so weitergeht als wäre nichts gewesen. Dafür muss eine hochwertige, zertifizierte Sicherheitssoftware – auch zur Überwachung der Datenein- und Ausgänge (Internet) vorhanden sein, und korrekt genutzt werden.
Erst wenn regelmäßige Vollsicherungen durch differenzielle und inkrementelle Datensicherungen ergänzt werden, kann man davon ausgehen, das eine im Verlustfall notwendige Datenwiederherstellung erfolgreich abläuft.

Inbetriebnahme neuer Geräte

Da zunehmend drahtlose Geräte in Netzwerken eingesetzt werden, muss bei der Inbetriebnahme darauf geachtet werden, dass die Sicherheitsmechanismen nicht aus Versehen deaktiviert bleiben. Viele Herstellen haben daher bereits bei der Lieferung von z.B. Routern eine Standardsicherheitseinstellung vorgegeben, die allerdings zum optimalen Nutzen der Anwender umgehend individualisiert werden sollte. Gemäß neuester Rechtsprechung macht sich niemand mehr strafbar, wenn er wissentlich oder unbeabsichtigt Zugang zu einem WLAN erhält und dieses auch nutzt.

In allen Fällen sind die Fachbetriebe des Informationstechniker-Handwerks die geeigneten Ansprechpartner wenn es darum geht, dem Thema Datensicherheit die entsprechende Beachtung zu schenken.
H.A. Kleiske