Sicherheit am Computer

Dieser Leitfaden orientiert den Anwender, wie er die tägliche Arbeit mit dem Personal Computer so sicher und zuverlässig wie möglich gestalten kann. Die empfohlenen Massnahmen können vom Benutzer selbst oder von einem IT-Verantwortlichen realisiert werden.

Internet

Hardware-Firewall
Eine Firewall sorgt für die Überwachung des Internetverkehrs und blockiert unerwünschte Zugriffe auf Computer oder Netzwerke. Hardware-Firewalls sind elektronische Geräte, die entweder direkt in Modems/Router integriert, oder als separate Einheit installiert werden. Sie sind sicherer und leistungsfähiger al sogenannte "Software- oder Personal-Firewalls". Hardware-Firewalls werden in der Regel von einem Neztwerkadministrator oder IT-Supporter installiert.

Antivirus-Programm auf Computer
Das Antivirus-Programm überprüft den lokalen Computer auf gefährliche Programme, sog. Malware. Je nach Hersteller werden auch eingehende E-Mails und andere Anwendungen überwacht. Bei der Anschaffung eines Antiviren-Programms sollte man auf eine möglichst geringe Auslastung der System-Ressourcen, sowie auf die Art der Lizenzierung achten. Damit Antiviren-Programme optimal arbeiten, sollten sie korrekt konfiguriert werden.

Surf-Verhalten
Generell gilt: Auf Geschäftscomputern sollte nur so wenig wie nötig gesurft werden. Unbekannte Websites und solche mit anstössigem oder verdächtigem Inhalt (Gewalt, Erotik, Gratis-Angebote) sollten unbedingt vermieden werden. Eine gesunde Portion Misstrauen ist beim Surfen im Internet nie fehl am Platz. Wenn die Option besteht, sollte man sich von geschützten Bereichen immer korrekt ausloggen/abmelden. (z.B. Webmail, Warenkorb, usw.)
Websites mit ungültigem oder fehlerhaftem Zertifikat sollten nicht besucht werden.

Umgang mit E-Mails
Auch beim Lesen und Verwalten von E-Mails ist Vorsicht geboten. Nachrichten mit verdächtigem oder fehlendem Betreff sofort löschen! Stammen diese Nachrichten von einer vertrauten Person, so kann ein kurzes Telefonat mit dem Betreffenden Klärung verschaffen. Nachrichten von staatlichen Behörden, öffentlichen Institutionen, Versicherungen oder Banken sollten nur dann geöffnet werden, wenn diese auch erwartet werden. Unerwartete Nachrichten dieser Absender sind meist gefälscht. Wichtige Korrespondenz muss von Gesetzes wegen ohnehin per Briefpost versandt werden. Ferner sollten Vorschaufenster oder Lesebereiche in E-Mailprogrammen deaktiviert werden, da sie eine grosse Sicherheitslücke darstellen.

Soziale Netzwerke
In sozialen Netzwerken, wie z.B. Facebook, Xing oder Google+ solle man sich gut überlegen, welche persönlichen Daten man preisgibt. Ansonsten gilt auch hier: Eine gesunde Portion Vorsicht gegenüber Freundschaftsanfragen, Nachrichten, Werbebanner, usw. ist immer angebracht.

Lokaler Computer

Passwörter
Kennwörter bestehen idealerweise aus einer Mischung von Buchstaben, Zahlen und Sonderzeichen. (Gross- und Kleinschreibung beachten!) Passwörter sollten grundsätzlich nicht auf Zettel geschrieben werden. Wer viele verschiedene Passwörter verwaltet und diese auf Papier notiert, sollte das Dokument sicher und wenn möglich verschlossen aufbewahren. Diese Punkte gelten übrigens auch für Passwörter, die im Internet verwendet werden.

Auf dem Computer installierte Software
Grundsätzlich gilt: Weniger ist mehr. Besonders auf geschäftlich verwendeten Computern sollte nur das installiert werden, was wirklich zum Arbeiten benötigt wird. Spielereien und dergleichen haben auf Business-PC's nichts zu suchen. Die Installation und Deinstallation von Software sollte immer ein Administrator oder ein Supporter vornehmen.

Datei-Management
Die Organisation von Daten ist essentiell. Ohne geht es nicht. Deshalb sollte jeder Anwender ein Konzept zur Erstellung, Verwaltung und Sicherung von Daten haben. Solche Konzepte können, wo mehrere Mitarbeiter an Computern arbeiten, auch von einem Gremium oder einem IT-Verantwortlichen festegelegt werden. Wichtig ist, dass sich jeder Benutzer an die Konventionen zum Umgang mit Daten hält. Fehlt das nötige Know-How, sollte unbedingt eine Schulung für die betreffenden Personen angeboten werden. Daten-Management ist auch in einzelnen Anwendungen wie z.B. E-Mail-Programmen von grosser Bedeutung.

Arbeitsplatz
Beim Verlassen des Arbeitsplatzes sollte sich der Benutzer abmelden, damit Unbefugte keinen Zugriff auf sensitive Daten haben. Unbekannte USB-Sticks sollten auf keinen Fall benutzt, sondern zuerst dem IT-Verantwortlichen gezeigt werden. Gerade aufgrund infizierter USB-Sticks wurde in den letzten Jahren massiver Schaden angerichtet.