1. GRUNDSÄTZLICHES

- Sicherheitsmaßnahmen sollten in Relation zu dem zu schützenden Gut stehen, wie z.B. Keine Alarmanlage für ein 12 Jahre altes Massenauto.
- Es gibt keine absolute Sicherheit im Internet.

2. ART DER GEFAHREN

Was	Erklärung Bedrohung/Gefahr Verbreitung	Gegenwehr Vorbeugung
Viren	Ein Programm das sich selbst verbreitet und eine Schadensroutine enthält. Braucht immer ein Wirtsprogramm (eine Datei) und kann nicht eigenständig „existieren“. Ändern, Löschen von Dateien. Ändern, Löschen von Datenbeständen. Infizieren anderer Rechner d.h. automatische Weiterverbreitung über Disketten, CD´s, Internet (Browser), Internet E-Mail, Rechnernetze (Intranet)	Antivirenprogramm(e) (Viren-scanner). Regelmäßige Datensicherung.
Würmer	Ein eigenständiges Programm das sich selbst per das Internet auf andere PC´s verbreitet und eine Schadensroutine enthält. Infiziert nicht andere Dateien. Ändern, Löschen von Dateien. Ändern, Löschen von Datenbeständen. Weiterverbreitung über Internet E-Mails, Rechnernetze (Intranet)	Antivirenprogramm(e), Firewall. Regelmäßige Datensicherung.
Trojaner	Ein eigenständiges Programm das neben der richtigen Funktion eine weitere unbemerkte Funktion enthält. Kann sich nicht selbst verbreiten, infiziert nicht andere Dateien. Ausspionieren und Weitergabe geldwerter Infos wie z.B. Passwörter, Kreditkarteninfos usw. Evtl. Ändern, Löschen von Dateien. Evtl. Ändern, Löschen von Datenbeständen. Wird oft vom Benutzer selbst aus dem Internet geladen und installiert. Über Rechnernetze (Intranet).	Antivirenprogramme (Viren-scanner), Personal Firewall, Antitrojanerprogramme. Regelmäßige Datensicherung.

Was	Erklärung Bedrohung/Gefahr Verbreitung	Gegenwehr Vorbeugung
Spyware, Adware	Ein Programm das den Benutzer ausspäht. Ist meist in Freewareprogrammen enthalten. Ausspionieren des Surfverhaltens, Ausspionieren und Weitergabe geldwerter Infos wie z.B. Userverhalten, persönliche Vorlieben usw. Wird vom Benutzer selbst aus dem Internet geladen und installiert.	Antispyware, Firewall.
Hacker	Angriff auf den PC, Aufdeckung von Sicherheitslücken, Ausspähung von Daten und Infos. Aufdeckung von Sicherheitslücken wird oft von systemkritischen Freaks (z.B. Chaos Computer Club) gemacht.	Regelmäßige Datensicherung. Firewall.
Unzuverlässige Betreiber	Daten (z.B. Kreditkarten Nr.) auf dem Server des Betreibers sind unzureichend gesichert und können von Unbefugten ausgelesen werden.	Keine geldwerten Infos weitergeben bzw. nur an „zuverlässige“ Partner
E-Mailinhalt wird gelesen	Der Inhalt einer E-Mail ist unsicherer als eine Postkarte die auf dem normalen Weg verschickt wird.	Verschlüsselung der E-mail z.B. mit PGP

3 VORBEUGENDE MAßNAHMEN

- Sicherheitseinstellungen am PC vornehmen
  - Im Bios des PC die Virenüberwachung einschalten
  - Windowsdateien wie z.B. win.ini usw. Schreibschutz (Schreibgeschützt) einschalten.

- Systemsicherheit
  - Unter WIN-NT, WIN2000, WINXP nie als Administrator arbeiten, immer als Benutzer am Rechner anmelden.
  - Vernünftiges Passwort suchen (Passwortstrategie)
    - keine Namen, Städte d.h. kein Wort das in einem Lexikon vorkommt.
    - Passwort lang genug (mind. 8 Stellen).
    - Im Passwort auch Sonderzeichen wie z.B.: !%(* usw.
  - Passwort(e) NIE AUF DER FESTPLATTE SPEICHERN !!!
  - Unbedingt alle Servicepatches einspielen, z.B. bei WIN2000 derzeit (Stand Jan. 2002) SP2 einspielen, bei WIN NT 4.0 ist es SP6a

- Netzwerkeinstellungen
  - TCP/IP nur für DFÜ verwenden.
  - Bei TCP/IP Dateifreigabe und Druckerfreigabe in jedem Fall deaktivieren.
  - Wenn Dateien oder Dateiverzeichnisse freigegeben werden müssen dann nur über Passwort erlauben.

- E-Mailsicherheit
  - Sicherheitseinstellungen im E-Mailclient vornehmen.
  - E-Mail Client regelmäßig updaten, regelmäßig E-Mail Client Patches einspielen.
  - Keine unbekannten E-Mails annehmen (von dubiosen Absendern, mit dubiosen Betreffs, ..)
  - E-Mailanhänge zuerst scannen mit Antivirusprogramm, dann lesen. Dazu natürlich zuerst herunterladen. E-Mailanhänge nie durch Doppelklick in Mailprogramm lesen !!!!!
  - Wenn möglich E-Mails nicht als HTML Mail lesen.
  - Wenn nötig E-Mails verschlüsseln. Hier bietet sich PGP an. Allerdings sollten dann alle E-Mails verschlüsselt werden.

- Browsersicherheit
  - Sicherheitseinstellungen im Browser vornehmen.
  - Browser regelmäßig updaten, regelmäßig Browser-Patches einspielen.

- Programmsicherheit (Word, EXCEL, usw.)
  - Macrovirusprotection in den entsprechenden Einstellungen einstellen.
  - Sicherheitsupdates (Service Packs und Patches) regelmäßig einspielen.

- Internetprogramme wechseln (zu „sichereren“ gehen)
  - Evtl. von MS-Outlook bzw. MS-Outlook auf einen sicheren E-Mailclient wechseln. Z.B. auf Pegasus Mail www.pmaild.com (deutsche Version, frei).
    Eudora Mail www.eudora.com (Frei, aber Werbeeinblendungen, gegen Zahlung werbefrei).
  - Evtl. von IE auf Opera Browser gehen www.opera.com (Frei aber Werbeeinblendung, gegen Zahlung werbefrei).
- Datensicherung
  - Datensicherungsstrategie (täglich ? Wöchentlich ? bei Bedarf ?) festlegen.
  - Regelmäßig Ihre Daten sichern.
  - Prüfen ob die gesicherten Daten auch lesbar sind.

- Virenscanner, Antivirenprogramm
  - Mindestens ein, besser zwei Programme einsetzen. Der Erkennungsgrad auch des besten Programms erreicht nicht 100% d.h. es erkennt nicht alle Viren.
  - Programme nach der Installation richtig konfigurieren.
  - Programme regelmäßig updaten, Virensignaturen regelmäßig updaten.

- Firewall
  - Die Installation bzw. der Einsatz einer Firewall ist ein Muß !!
  - Firewall nach der Installation richtig konfigurieren, besser zu restriktiv als zu großzügig.
  - Firewall regelmäßig updaten.
  - Das / die Logfiles der Firewall unbedingt regelmäßig anschauen wer wie in Ihren Rechner eindringen will, welche Programme ins Internet gehen wollen.

4. WAS TUN BEI VIRENBEFALL / WURMBEFALL / TROJANERN / SPYWARE

4.1 Virenbefall / Wurmbefall

- Ruhe bewahren.
- Rechner über die (hoffentlich vorhandene) Bootdiskette für DOS booten, geht nur bei FAT und FAT32 er Filesystem.
  ACHTUNG: Bei NTFS Filesystem ist dies etwas komplizierter.
- Mit dem hoffentlich vorhandenen Virenscanner das System scannen.
- Infizierte Dateien reparieren (wenn möglich) sonst löschen.
- Bei Befall mit nur einem Virus / Wurm wie z.B. NIMDA evtl. mit einem anderen Rechner Wurm / Virenentfernungsprogramme aus dem Internet laden und auf dem infizierten Rechner laufen lassen.

- Wenn keine Systemdateien betroffen sind System wieder hochfahren.
- Mit einem zweiten Virenscanner System erneut scannen.
- Im schlimmsten Fall (das ist der sicherste aber aufwändigste Weg) Harddisk neu formatieren, danach System und Programme neu installieren.
  Anschließend unbedingt die Datenträger mit den Backups vor dem Einspielen auf Viren/Wurmbefall prüfen.

4.2 Befall mit Trojaner
- Aus dem Internet Antitrojanerprogramm runterladen.
- Rechner damit scannen.
- Trojaner entfernen bzw. wenn in einem Programm verborgen dieses Programm entfernen.

4.3 Verdacht auf Spyware
- Aus dem Internet Antispywareprogramm runterladen.
- Rechner damit scannen.
- Antispywareprogramm entfernen bzw. wenn in einem Programm verborgen dieses Programm entfernen.
  Ein anderer Weg ist auch diesem Programm über die Firewalleinstellung den Zugang zum Internet verbieten.

5. GRUNDSÄTZLICHES ZU INTERNET BANKING, INTERNET EINKAUF (ONLINE EINKAUF), E-MAIL

INTERNET BANKING, INTERNET EINKAUF
- Verbindungen zur Bank/zum Händler (Onlineshop) sollten immer über SSL gehen (der Browser zeigt in der Taskleiste ein kleines Schloss bzw. einen kleinen Schlüssel an).
- SSL ist relativ sicher wenn es auf der Anbieterseite (Server der Internetbank, Server des Onlinehändlers) richtig implementiert wurde.
  Allerdings sagt die Sicherheit der Übertragung nichts aus über die Sicherheit der Daten auf dem Server selbst.
  In den Medien ist ab und an zu lesen dass z.B. wieder von zig Kunden die Kreditkartendaten auf dem Server frei zugänglich waren, dass Passwörter der Kunden auf einem Server von jedem lesbar war, dass in Amerika Kundendaten eines bankrott gegangenen Betreibers verkauft wurden usw.
  IM KLARTEXT:
  Egal wie sicher Sie Ihren PC machen, egal wie sicher die Datenübertragung von Ihnen zum Onlineshop, zum Bankinstitut ist, Sie haben keinen Einfluß darauf was mit Ihren Daten auf diesen Servern passiert.
  Sie selbst müssen also entscheiden ob Sie Onlineshopping und Onlinebanking nutzen wollen.

E-MAIL
- Die Absenderangaben einer E-Mail sind kinderleicht zu fälschen.
- Der Inhalt einer E-Mail ist kinderleicht zu fälschen.
- Es ist einfach eine E-Mail unter falschem Absender zu verschicken.
- Der Inhalt einer E-Mail ist unsicherer als eine Postkarte, d.h. viele können die E-Mail lesen.
- Es gibt E-Mailanbieter z.B. WEB.DE welche die E-Mailübertragung über SSL abwickeln. Damit werden Passwort und/oder Mailinhalt auf dem Weg vom Mailclient (dem Anwender) zum E-Mail Server verschlüsselt. Allerdings unterstützen nur wenige E-Mailclients, darunter der Netscape Messenger diese Technik.
- Eine Verschlüsselung der E-Mail ist z.B. über das gute und für den Privatgebrauch kostenlose Verschlüsselungsprogramm PGP möglich.

6. ONLINE SICHERHEITSTESTS DES COMPUTERS

http://www.ita.hsr.ch/cgi-bin/datenschutz/DSZ_test_start.html
Schweizer Datenschutzbeauftragter (Hochschule Rapperswill CH)

http://www.lfd.niedersachsen.de/service/service_selbstt.html
Der Landesbeauftragte für den Datenschutz Niedersachsen

http://secutity1.norton.com
Antivirenscanner Hersteller