Verhaltensempfehlungen im Umgang mit Internet & E-Mail

Einleitung

Die folgenden Richtlinien und Verhaltensempfehlung sind dazu geeignet, bösartige Programme, wie Viren, Würmer und Trojanische Pferde, von Personal Computern fernzuhalten.

Viren sind entweder Programme oder Makros, die auf einem befallenen System beliebige Aktionen auslösen können, z.B. Starten von Programmen, löschen oder verändern von Dateien etc.

Würmer sind Programme, deren Hauptaufgabe es oft ist, sich möglichst schnell weiterzuverbreiten. Trotzdem können sie beliebiges Schadenspotenzial enthalten. Sie lösen häufig eine enorme Flut von E-Mails aus, in denen sie sich selbst als Anhang an alle E-Mail Adressen verschicken, die sie auf dem betroffenen Computer finden.

Trojanische Pferde (oder Backdoor-Programme) sind die unangenehmsten Vertreter so genannter Malware, also bösartigen Codes. Sie richten sich meist dauerhaft auf dem infizierten System ein, spionieren den Anwender aus (z.B. Kreditkartennummern) oder öffnen Hintertüren für ev. noch viel bösartigere Software.

Schadsoftware gelangt i.d.R. als Anhang in elektronischer Post auf das System, oder über Wechselmedien, wie USB-Speicher, Speicherkarten und CDs & DVDs. Infektionen sind aber auch über Downloads und kontaminierte Webseiten möglich.

Tipps zum Schutz vor Viren, Würmer & Trojanischen Pferden

Durch das Beherzigen einiger weniger Ratschläge kann man sich recht zuverlässig vor Computerviren schützen. Diese ersetzten keine Antivirenprogramme, kosten kein Geld, können sich aber sehr positiv auf Datensicherheit und Datenschutz auswirken.

1. Betriebssystem und Anwendungssoftware auf aktuellem Stand halten. Aktualisierungen von Microsoft (Windows & Office) und Adobe (Flash Player & Adobe Reader) möglichst sofort installieren.
2. Regelmässig und häufig Daten sichern. Das gilt zumindest für Daten und Dokumente. Auch sinnvoll bei Hardwaredefekten!
3. Keine Chance für Bootviren durch Änderung der Bootsequenz im BIOS des PC (interne Festplatte an erster Stelle) und das Entfernen von USB-Speichern und CDs aus dem Laufwerk vor dem Ausschalten des Computers.
4. Fremder Software misstrauen. Nur Software aus seriösen Quellen einsetzen. Keine Raubkopien verwenden. Keine Programme starten, die über E-Mail versandt wurden. Fremde Datenträger und aus dem Netz herunter geladene Software mit einem Virenscanner prüfen.
5. Rechner vor fremdem Zugriff schützen, z.B. mit Bildschirmschoner mit Passwort, BIOS-Passwort beim Systemstart und Blockierung bei Abwesenheit (Windowstaste + L).
6. Neugier zügeln. Beispielsweise riecht ein Link zu einer Seite mit dem Titel "Jennifer Lawrence nackt" förmlich nach einer Falle. Der Besuch einer solchen Internet-Seite kann ungeahnte Folgen haben.

Sinnvolle Verhaltensregeln

Was sollte man unbedingt lassen?

- Passworte abspeichern.
- Programme aus dubiosen Quellen herunterladen und installieren.
- Anhänge aus E-Mails bekannter und unbekannter Herkunft öffnen, bzw. starten. Besonders trifft das auf Dateien mit den Endungen .exe, .scr und .zip zu.
- Anfragen nach Benutzerkennung und Passwort beantworten (telefonisch oder per E-Mail).
- Ketten E-Mails weiterverbreiten.

Was darf man (einigermassen) bedenkenlos tun?

- E-Mails aus seriösen und bekannten Quellen öffnen (gilt nur beschränkt für Anhänge). In sog. HTML E-Mails (Mails mit Proportionalschrift und sofort sichtbaren Grafiken) kann sich auch unerwünschter Code befinden, nur reine Text-Mails sind vollkommen ungefährlich.
- Dateien (Bilder und Dokumente) aus dem Internet herunterladen und mit einem Viewer ansehen.

Was sollte man sich gut überlegen?

- Öffnen von Anhängen (Dokumente und besonders ausführbare Dateien) aus E-Mails von unbekannten Absendern. Besser zuerst auf die Festplatte speichern (Rechtsklick – Speichern unter …), auf Schadcode überprüfen oder mit einem Viewer betrachten.
- E-Mails öffnen, wenn sie eigenartige Titel oder Absender tragen. Daraus entsteht selten ein Schaden! Schadcode kann sich im HTML-Code verstecken und durch das blosse Öffnen eines Mails aktiviert werden. Im Zweifelsfall also: E-Mail ungeöffnet löschen, wenn es etwas Wichtiges war, wird sich der Absender nochmals melden! Diese Arten von Nachrichten sind sehr oft in Englisch oder katastrophalem Deutsch abgefasst. Erhöhtes Misstrauen bei "eigenartigem" Betreff!
  In diesem Zusammenhang wichtig: Bei aktiviertem Lesebereich wird die Nachricht bereits durch einfaches Anwählen geöffnet – besser ausschalten!
- Wenn im Internet-Browser beim Anklicken eines Links das Fenster "Dateidownload" erscheint, bitte genau nachsehen, was herunter geladen werden soll. Falls die Datei erwünscht ist, unbedingt "Speichern" wählen und vor dem Öffnen mit dem Virenscanner überprüfen. Niemals direkt "Öffnen" anklicken, damit wird eine ausführbare Datei sofort gestartet!
- Passworte abspeichern. Widerstehen Sie dem Häkchen vor oder unter "Angemeldet bleiben", "Kennwort merken", "Anmeldedaten speichern" und dergleichen.

Präventive Massnahmen

Gesundes Misstrauen ist im Umgang mit E-Mail und Internet auf jeden Fall angebracht. Durch die Berücksichtigung der Ratschläge in diesem Dokument ist die Gefahr einer Ansteckung bereits sehr stark reduziert. Zusammenfassend sind folgende präventive Massnahmen sinnvoll:

- Vorsicht mit Dokumenten aus unbekannten Quellen.
- Keine Programme aus dubiosen Quellen installieren (Internet, CD oder USB-Speicher).
- Regelmässig Sicherheitsupdates für alle wichtigen Programme installieren.
- Installation eines modernen Virenscanners, Sicherstellung regelmässiger Aktualisierung der Virensignaturen und regelmässige Virenprüfung der lokalen Laufwerke.

Zusammenfassung

- Absolute Sicherheit gibt es nicht!
- Bitte misstrauisch & vorsichtig sein. Lieber eine Nachricht zu viel als zu wenig löschen und die Neugierde bei zugesandten Internet-Links zügeln!
- Der Anwender kann sehr viel zur Sicherheit eines IT-Netzwerks beitragen!