Verhaltensempfehlungen im Umgang mit Internet & E-Mail

Einleitung

Die folgenden Richtlinien und Verhaltensempfehlung sind dazu geeignet, bösartige und unerwünschte Programme möglichst von Personal Computern und Netzwerken fernzuhalten.

Das 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.

Teilweise sind es auch Programme, deren Hauptaufgabe es ist, sich möglichst schnell weiterzuverbreiten. Trotzdem können sie beliebiges Schadenspotenzial enthalten.

Sie richten sich meist dauerhaft auf dem infizierten System ein, spionieren den Anwender aus (z.B. Kreditkartennummern, E-Mail Verkehr) oder öffnen Hintertüren für den eigentlichen Angriff.

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.

Sie werden es gleich feststellen: Sicherheit ist kein Selbstläufer! Um Sicherheit muss man sich bemühen und die notwendige Sensibilität für Gefahren entwickeln.

Letztlich sind immer Sie es, der/die entscheidet, ob Sie eine Einladung annehmen, eine Datei öffnen oder einen Link anklicken. Die Technik kann danach nur noch versuchen, das Schlimmste zu verhindern!

Mehr Sicherheit bedeut immer weniger Komfort und ist anstrengend!

Tipps zum Schutz vor Schaden aus dem Internet

Durch das Beherzigen einiger weniger Ratschläge kann man sich einigermassen zuverlässig vor Schäden schützen. Diese ersetzten keine Antivirenprogramme, kosten kein Geld, können sich aber sehr positiv auf die Sicherheit von Informatik-Infrastrukturen auswirken.

1. Betriebssystem und Anwendungssoftware auf aktuellem Stand halten. Aktualisierungen von Microsoft (Windows & Office) und Adobe (Adobe Reader) möglichst sofort installieren.
2. Regelmässig und häufig Daten sichern. Das gilt zumindest für Daten und Dokumente. Auch sinnvoll bei Hardwaredefekten!
3. Fremder Software misstrauen. Nur Software aus seriösen Quellen einsetzen. Keine Raubkopien verwenden. Keine Programme von unseriösen Quellen starten. Fremde Datenträger und aus dem Netz heruntergeladene Software mit einem Virenscanner prüfen.
4. Rechner vor fremdem Zugriff schützen, z.B. mit Bildschirmschoner mit Passwort und Blockierung bei Abwesenheit (Windowstaste + L).
5. Neugier zügeln. Beispielsweise riecht ein Link zu einer Seite mit dem Titel "Gewinnen Sie sofort 1 Million" förmlich nach einer Falle. Der Besuch einer solchen Internet-Seite kann ungeahnte Folgen haben.
6. Misstrauisch sein! Nachrichten mit eigenartigem Inhalt löschen oder zumindest hinterfragen.
   Wichtig: Rückfragen unbedingt auf einem anderen Informationskanal, denn eine E-Mail Adresse könnte gefälscht oder ein Konto (E-Mail, WhatsApp etc.) gekapert sein.
7. Lieber einmal zu viel zögern, als einmal zu wenig. Lassen Sie sich nicht unter Druck setzen (zeitlich oder durch Veröffentlichungsdrohungen).
8. Seien Sie sparsam mit persönlichen Daten. Geben Sie Ihre E-Mail Adresse nicht leichtfertig preis, bestellen Sie in Internetgeschäften wenn möglich als Gast und hinterlegen Sie Ihre Kreditkartendaten möglichst nicht.
   Es nützt Ihnen nichts, wenn Sie sich an alle Empfehlungen halten, sich der Geschäftsbetreiber Ihre Daten aber stehlen lässt!
9. Nehmen Sie nicht mehr unterstützte Hard- & Software ausser Betrieb.

Empfohlenes Verhalten

Was sollte man unbedingt lassen?

- Passworte abspeichern.
- Programme aus dubiosen Quellen herunterladen und installieren.
- Anhänge aus E-Mails bekannter und unbekannter Herkunft öffnen. Besonders trifft das auf MS Office-Dateien und ZIP-Archive zu.
- Anfragen nach Benutzerkennung und Passwort beantworten (telefonisch oder per E-Mail).
- Links in E-Mails anklicken, besonders in solchen von unbekannten Absendern.

Was darf man (einigermassen) bedenkenlos tun?

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

Was sollte man sich gut überlegen?

- Öffnen von Anhängen in E-Mails von bekannten und unbekannten Absendern. Besser zuerst auf die Festplatte speichern (Rechtsklick – Speichern unter …), auf Schadcode überprüfen oder mit einem Viewer betrachten. Im Zweifelsfall nachfragen!
- E-Mails öffnen, wenn sie eigenartige Titel oder Absender tragen. Schadcode kann sich im HTML-Code verstecken und durch das blosse Öffnen einer Nachricht 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 immer öfters auch in einwandfreiem 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 heruntergeladen 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. Zusammenfassend sind folgende präventive Massnahmen sinnvoll:

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

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!