ICHECK*S NETZ

5

Computersicherheit & Passwörter

1. Malware

- **Spuren -** Sobald der Rechner eine Online-Verbindung herstellt, empfängt und sendet er Daten und hinterlässt Spuren.
- **Begriff -** Malware ist der Oberbegriff für Software, die dem Anwender schaden kann. Damit sind Computerviren, E-Mail-Würmer, Trojanische Pferde, Einwählprogramme (Dialer) und Spyware gemeint.
- **Ansteckung -** Diese Programme gelangen in den PC:
  - über infizierte Speichermedien (z.B. USB – Stick);
  - beim Öffnen verseuchter E-Mail – Dateianhänge;
  - durch das Herunterladen und Installieren von Software.

Computersicherheit & Passwörter

- **Was sind Viren?** Ein Computervirus ist ein Programm, das auf einem Rechner Schäden an Soft- und Hardware anrichten- und sich massenhaft verbreiten kann.
- **Was sind Trojaner?** Trojanische Pferde schleichen sich als vermeintlich nützliche Programme getarnt in einen Computer ein (meistens über Anhänge in E-Mails) und können die Kontrolle und Steuerung des befallenen Computers von außen übernehmen.
- **Was ist Spyware?** Diese Programme „spionieren“ private Daten oder das Surfverhalten aus und geben diese Informationen unbemerkt an Dritte weiter

Computersicherheit & Passwörter

2. Viren, Trojaner und Spam: es geht ums Geld!

- **Parasiten -** Heutige Virengenerationen löschen keine Festplatten oder Dateien mehr. Sie schaden nicht mehr ihrem Wirt – demjenigen, der den Virus hat.
- **Adressensauger -** Vielmehr sammeln sie auf den verseuchten Computern E-Mail-Adressen oder sie versenden von dort zigtausend Spams an andere Computer. Auch andere Missbrauchsmöglichkeiten sind denkbar.
- **Ferngesteuert -** Die befallenen Rechner sind für Hacker völlig offen und können von außen gesteuert werden, ohne dass die Benutzer etwas davon merken. Warum das alles? Um viel Geld zu verdienen!

Computersicherheit & Passwörter

A) Wie kann ich mich vor Viren schützen?

- **Nicht downloaden –** Unbekannten Dateianhänge (Attachments) von E-Mails weder herunterladen, noch öffnen, noch ausführen! Attachements können aber auch von bekannten Absendern stammen, da sich Viren über die Adressbücher der befallenen Rechner selbstständig weiterversenden.
- **Nicht ausführen -** Deaktiviere im Browser, im E-Mail-Programm und im ZIP-Programm die Voreinstellung, dass heruntergeladene Dateien sofort ausgeführt werden. Solltest du nämlich doch versehentlich einen Virus auf deiner Festplatte haben, dann wird dieser erst aktiv, wenn das Programm ausgeführt wird.

Computersicherheit & Passwörter

B) Beachte vier wichtige Punkte

- **Software updaten –** Erstens: Anwendungsprogramme und Betriebssysteme weisen immer wieder Sicherheitslücken auf, die erst mit der Zeit ausfindig gemacht werden. Darum ist es wichtig, dass du die automatischen Software – Updates aktivierst und regelmäßig durchführst.
- **Firewall –** Zweitens: eine elektronische „Brandschutzmauer“ ist im Betriebssystem integriert und muss nur aktiviert werden. Sie verhindert gefährliche Zugriffe aus dem Internet auf deinen Computer. Firewalls sind als Software- oder als Hardware erhältlich.

Computersicherheit & Passwörter

- **Antivirus –** Drittens: verwende ein Antivirus–Programm. Es schützt deinen Computer aber nur dann, wenn du es regelmäßig aktualisierst. Alle Virenschutzprogramme bieten eine automatische Aktualisierung an, die du unbedingt nutzen solltest. Dabei werden die neuesten Informationen über bekannte Schadprogramme vom Server des Antivirus – Anbieters heruntergeladen. :
- **Antispyware –** Viertens: Spyware ist eine besondere Art Schadproramm. Es erfasst unbemerkt persönliche Daten auf deinem Computer und leitet sie über das Internet weiter. Du solltest zusätzlich zum Antivirus auch ein Antispyware – Programm verwenden.

Computersicherheit & Passwörter

3. Aktive Inhalte

- **Mehr Effekte –** Aktive Inhalte sind Programmteile, die im Internetbrowser versteckt sind. Sie ermöglichen, dass im Internet-Browser schöne, multimediale Effekte und Spezialfunktionen angezeigt werden. Verbreitete Technologien sind: ActiveX, JavaScript und VBScript.
- **ActiveX -** Das ist ein von Microsoft entwickelter aktiver Inhalt. ActiveX sorgt dafür, dass die Windows-Anwendungen mit dem Internet zusammenarbeiten. Die Nutzer haben aber keine Kontrolle darüber, was aktive Inhalte auf dem Rechner machen. Ihr Funktionsumfang kann weder kontrolliert noch eingeschränkt werden. Darum stellt das ActiveX ein Sicherheitsrisiko dar.

Computersicherheit & Passwörter

4. Ist dein Computer ferngesteuert?

- **Bots –** Könnte es sein, dass dein Computer für einen anderen Computer arbeitet – ohne dass du es merkst. Bots heißen die Programme, die sich in deinem Computer einnisten und das bewirken. Bots werden eingesetzt, um z. B. Spam unerkannt zu versenden. Dazu werden mehrere hunderte oder tausende Computer zu Bot-Netzen verbunden. Sie verhalten sich so lange unauffällig, bis sie ferngesteuert aktiviert werden und die schädlichen Aktionen ausführen.
- **Illegale Geschäfte -** Bot-Netze werden oft an Dritte weitervermietet. Hinter Bots steckt ein Geschäftsmodell – und viel kriminelle Energie.

Computersicherheit & Passwörter

5. Unsichere Passwörter sind bald geknackt!

- **Sichere Passwörter enthalten:**
  - zumindest sechs bis acht Buchstaben;
  - Groß- und Kleinbuchstaben;
  - Zahlen und Sonderzeichen (- * \ : " / usw.).
- **Eselsbrücken -** Pass auf, dass dich bei der Passworteingabe niemand beobachtet! Passwörter merkst du dir am besten durch Eselsbrücken.
  Beispiel: „IbeFvTH!“:
  Lösung: **„I**ch **b**in **e**in **F**an **v**on **T**okyo **H**otel**!**“.

Computersicherheit & Passwörter

- **Konzentriere dich! -** Benutze Zeichenfolgen, die niemand erraten kann und ändere von Zeit zu Zeit dein Passwort. Wenn du dir Passwörter nicht merken kannst und sie aufschreibst, musst du folgendes beachten:
  - Passwort nicht als Passwort bezeichnen;
  - Nicht direkt am Computer aufbewahren.

Computersicherheit & Passwörter

6. Worauf sollst du bei öffentlichen Computern achten?

- **Öffentliche Computer -** Sind Computer in der Schule, Internetcafés, Bibliotheken, Bahnhöfen und anderen öffentlichen Orten sicher? Das hängt davon ab, wie du dort mit deinen persönlichen Daten umgehst.
- **Lass niemanden zuschauen –** Achte bei der Eingabe persönlicher Daten darauf, dass dir niemand zuschaut.
- **Gib nicht zu viele persönliche Daten ein –** denn du bis auch vor Gelegenheitshackern nicht sicher, die nach dir denselben öffentlichen Computer benutzen könnten. Bank- oder Kreditkartendaten oder ähnlich vertrauliche Informationen solltest du nie auf einem öffentlichen Rechner eingeben.

Computersicherheit & Passwörter

- **Lass den Computer nicht unbeaufsichtigt –** Wenn du fertig bist, melde dich bei allen Websites und Programmen ab.
- **Seichere nie deine Login Daten -** Ein Beispiel: du bist auf einer Website zum Checken deiner E-Mails eingeloggt. Melde dich immer mit Klick auf „Logout“ oder „Abmelden“ ab. Deaktiviere auch automatische Anmeldefunktionen (z.B. bei Instant Messengern)
- **Beseitige alle Spuren -** Die meisten Webbrowser merken sich automatisch deine Passwörter und jede Website, die du besucht hast. Klicke
  a) im Internet Explorer auf: „Extras / Internetoptionen“
  b) in Firefox auf: „Extras / Einstellungen / Datenschutz“
  und lösche dort alle deine Spuren.

Computersicherheit & Passwörter

7. Lokale drahtlose Funknetze

- **W-LAN –** Eine „Wireless Local Area Network“ - Karte ist im Rechner meistens schon eingebaut. Notwendig sind dann noch ein W-LAN-Router und ein Netzzugang.
  - Mache das W-LAN für Dritte unsichtbar (SSID – Senden ausschalten);
  - Aktiviere die Verschlüsselung deiner Daten (WPA, WPA2).
- **Netzeinwahl -** Wenn du ins W-LAN einwählst, dann:
  - Deaktiviere die Datei- und Verzeichnisfreigaben für Netzwerke;
  - Gib Daten nur über SSL-verschlüsselte Websites ein. Du erkennst du an „https://“ bzw. am Schloss-Symbol!

Computersicherheit & Passwörter

Check´s!

1. Was ist „Malware“ und was ist „Spyware“
2. Was ist ein „Virus“ und was ein „Trojaner“?
3. Wie kannst du dich vor Viren schützen?
4. Welche vier Punkte sind bei Viren und Trojanern zu beachten?
5. Was sind „Aktive Inhalte“?
6. Was sind „Bots“?
7. Aus welchen Bestandteilen besteht ein ein sicheres Passwort?
8. Worauf sollst du bei der Verwendung von öffentlichen Computern achten?
9. Wofür steht die Abkürzung W-LAN und was heißt „wireless“?

ICHECK'S NET(Z)

Landesberufsschule für Handel, Handwerk und Industrie
Dipl. Ing. Luis Zuegg
Meran