Merkblatt 12 (aktualisiert 7.6.18)

Computer Schädlinge (Auszug aus der Meldestelle des Bundes)

Viren
Viren gelangen häufig über Anhänge in E-Mails oder über infizierte Dateien, die vom Internet heruntergeladen werden, auf den Rechner. Einmal aktiviert, können sie sich auch per E-Mail an Kontakte im Adressbuch weiterversenden. Weitere Verbreitungswege sind externe Datenträger (z.B. CD-ROM, USB Memory Stick, usw.).

Würmer
Würmer bestehen, wie Viren, aus Programmanweisungen, die dem Rechner die auszuführenden Aktionen vorgeben.

Trojanische Pferde
Trojanische Pferde (häufig als Trojaner bezeichnet) sind Programme, die im Verborgenen schädliche Aktionen ausführen und sich dabei für den Benutzer als nützliche Anwendung oder Datei tarnen. Häufig sind Trojanische Pferde Programme, die im Internet heruntergeladen werden, oder über Anhänge in E-Mails verbreitet.

Spyware und Adware
Der Begriff "Spyware" setzt sich aus den englischen Wörtern "Spy" (Spion) und "Software" zusammen. Spyware soll ohne Wissen des Benutzers Informationen über dessen Surfgewohnheiten oder Systemeinstellungen sammeln und diese an eine vordefinierte Adresse übermitteln.
„Adware" setzt sich aus den englischen Wörtern "Advertising" (Werbung) und "Software" zusammen. Eine klare Definitionsgrenze zwischen Spyware und Adware ist schwer zu erkennen. Spy- bzw. Adware gelangt meist über heruntergeladene Programme auf den Rechner.

Phising
Das Wort Phishing setzt sich aus den englischen Wörtern "Password", "Harvesting" und "Fishing" zusammen. Mittels Phishing versuchen Betrüger, an vertrauliche Daten von ahnungslosen Internet-Benutzern zu gelangen. Dabei kann es sich beispielsweise um Kontoinformationen von Online-Auktionsanbietern (z.B. eBay) oder Zugangsdaten für das Internet Banking handeln. Die Betrüger nutzen die Gutgläubigkeit und Hilfsbereitschaft ihrer Opfer aus, indem sie ihnen E-Mails mit gefälschten Absenderadressen zustellen. In den E-Mails wird das Opfer beispielsweise darauf hingewiesen, dass seine Kontoinformationen und Zugangsdaten (z.B. Benutzernamen und Passwort) nicht mehr sicher oder aktuell sind und es diese unter dem im E-Mail aufgeführten Link ändern soll. Der Link führt dann allerdings nicht auf die Originalseite des jeweiligen Dienstanbieters (z.B. der Bank), sondern auf eine vom Betrüger identisch aufgesetzte Webseite.

Spam
Spam ist der Überbegriff für unerwünschte Werbemails oder Kettenbriefe. Als Spammer bezeichnet man den Verursacher dieser Mitteilungen, während das Versenden selbst als Spamming bezeichnet wird.

Cookies
Cookies sind kleine Textdateien, die beim Besuch einer Webseite auf dem Rechner des Webseitenbesuchers abgelegt werden. Sie werden eingesetzt, um die Arbeit des Benutzers zu erleichtern. Beispielsweise muss man sich bei einigen Online-Diensten mit Benutzernamen und dem entsprechenden Passwort anmelden. Um diese nicht jedes Mal neu eingeben zu müssen, werden solche Informationen bei Wahl einer entsprechenden Option in einem Cookie auf der lokalen Festplatte abgelegt und bei jedem Besuch der Seite automatisch in die entsprechenden Felder eingefügt.

Personal Firewall

Eine Firewall (engl. für Brandmauer) schützt Computersysteme, indem sie ein- und ausgehende Verbindungen überwacht und gegebenenfalls zurückweist. So gesehen ist eine Firewall mit einem Wachposten an einem Schlosstor zu vergleichen. Die Entscheidung, welche Verbindungen zugelassen oder zurückgewiesen werden, erfolgt anhand von einfachen Regeln, die bei jedem neuen Verbindungsaufbau abgefragt werden. Durch Firewalls kann das Risiko von unrechtmässigen Zugriffen durch Hacker (Computereindringlinge) gesenkt sowie die Gefahren von Trojanischen Pferden, Spyware oder Würmern minimiert werden.

- Personal Firewall einsetzen
  Wie Antiviren-Programme sind auch Personal Firewalls als Zusatzsoftware erhältlich und können teilweise kostenlos vom Internet heruntergeladen werden. Einige Betriebssysteme sind bereits mit einer Personal Firewall ausgestattet, die Sie nutzen sollten.
- Personal Firewall kommt vor dem Internet-Anschluss
  Wenn Ihr Rechner über ein Personal Firewall verfügt, so aktivieren Sie diese unbedingt bevor Sie den Rechner (zum ersten Mal) am Internet anschliessen. Das Herunterladen von Software Updates sowie weiteren Programmen und Dateien sollte nur bei aktivierter Personal Firewall erfolgen.

Software Updates

- Sicherheitsrelevante Software Updates (sogenannte Patches) schliessen Sicherheitslücken, welche beinahe täglich entdeckt werden. Sicherheitslücken können unrechtmässige Zugriffe auf Ihre Daten oder die Ausbreitung von Würmern ermöglichen und sind sowohl in Betriebssystemen, wie auch in Anwendungen vorhanden. Um die Sicherheit Ihrer Daten zu erhöhen, kommt dem Einspielen von Software Updates deshalb eine grosse Bedeutung zu.

- Regelmässige Updates von Betriebssystem und Anwendungen
  Einige Produkte stellen dazu eine automatische Update-Funktion zur Verfügung, die Sie unbedingt nutzen sollten. Überprüfen Sie regelmässig, ob diese aktiviert ist. Informationen zu aktuellen Software Updates sind in der Regel auf den Web-Seiten der jeweiligen Hersteller zu finden.

Antiviren Software

- Antiviren-Software schützt Ihre Daten vor Viren, Würmern oder Trojanischen Pferden. Eine aktuelle Antiviren-Software ist absolut unverzichtbar, wenn Sie Programme und Dateien vom Internet herunterladen oder mit anderen Personen austauschen. Da allein pro Tag mehrere neue Viren, Würmer oder Trojanische Pferde auftauchen können, ist eine häufige Aktualisierung der Antiviren-Software zwingend erforderlich.

- Installation von Antiviren-Software. Setzen sie unbedingt eine aktuelle Antiviren-Software ein.

- **Antiviren-Software regelmässig aktualisieren**. Stellen Sie sicher, dass die Antiviren-Software mindestens zwei bis drei Mal pro Woche aktualisiert wird. Die meisten Produkte verfügen über eine automatische Online-Update-Funktion, die Ihnen diese Arbeit abnimmt und unbedingt eingeschaltet werden sollte.

- Gültigkeit der Lizenz überprüfen. Vergewissern Sie sich regelmässig, ob die Lizenz der eingesetzten Antiviren-Software noch gültig ist. Zwar funktioniert die Software auch noch nach Ablauf der Gültigkeitsdauer. Allerdings können ab diesem Zeitpunkt keine Updates mehr bezogen werden.

- Benutzer von Windows 10 haben auf ihrem PC bereits den "Windows Defender" installiert, der sehr gute Resultate erbringt.

Datensicherung

- Es kann nie ausgeschlossen werden, dass Daten durch Fehlmanipulation, wegen technischer Defekte oder durch Viren beziehungsweise Würmer teilweise zerstört werden oder gar ganz verloren gehen. Um das Risiko eines Datenverlustes zu minimieren, ist die regelmässige Durchführung einer Datensicherung (Backup) dringend zu empfehlen. Am besten benutzen Sie eine externe Festplatte, die Sie nach der Sicherung wieder vom PC trennen.

Verhaltensregeln

- Neben technischen Massnahmen (z.B. Personal Firewall, Software-Updates, Antiviren-Software, usw.) zur Erhöhung der Sicherheit eines Rechners, ist vor allem das Verhalten jedes einzelnen Benutzers von entscheidender Bedeutung. Tipp: Gehirn einschalten.

Passwortwahl

- Sowohl Ihr Rechner wie auch unterschiedliche Online-Dienste verlangen die Vergabe eines Passwortes. Schlecht gewählte oder zu kurze - also schwache - Passwörter stellen ein erhebliches Sicherheitsrisiko dar. Bei der Wahl eines Passwortes sind die folgenden Grundsätze zu beachten:

- Mindestlänge von 8 Zeichen
  Die Mindestlänge des Passwortes sollte bei 8 Zeichen liegen und sowohl aus Buchstaben, Zahlen wie auch Sonderzeichen bestehen.

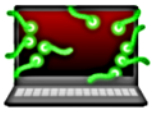
- Einfach zu merken. Das Passwort ist so zu wählen, dass man es sich einfach merken kann. Schreiben sie keine Passwörter auf.

MALWARE

Das Wort Malware setzt sich aus dem englischen Adjektiv „malicious" („bösartig", „schlecht") und dem Suffix „-ware" zusammen. Es ist der Oberbegriff für alle Arten von Schadprogrammen.

VIRUS

Der Virus ist ein Schädling, der in der Lage ist, sich selbst in Dokumente, Programme oder gar Datenträger zu kopieren. Die Schäden, die er anrichtet, betreffen in manchen Fällen auch die Hardware.



WURM

Ein Computerwurm funktioniert ähnlich wie ein Virus. Er breitet sich jedoch aus, ohne Dateien und Bootsektoren mit seinem Schadcode zu infizieren. Seine Strategie besteht darin, sich unauffällig im System einzunisten und möglichst keine sichtbaren Symptome zu verursachen.

BACKDOOR

Beim Backdoor handelt es sich um ein Schadprogramm, das unbefugten Personen ein Hintertürchen öffnet und ihnen damit den Zugriff auf den PC ermöglicht.

SPYWARE

Eine Spyware sammelt Informationen über das Userverhalten im Internet und sendet die gewonnenen Daten an ihren Entwickler. Dieser verkauft die Nutzer-Infos weiter oder verwendet sie selbst für gezielte Werbeeinblendungen.

TROJANER

Ein Trojaner ist ein Programm, das sich als nützliche Software ausgibt, im Hintergrund jedoch eine schädliche Funktion erfüllt. Oft installiert es andere Schädlinge wie Spywares oder Backdoors auf dem Ziel-PC.

SCAREWARE

Das Wort „Scareware" setzt sich aus dem englischen Verb „scare" („erschrecken", „ängstigen") und dem Suffix „-ware" zusammen. Eine Schadsoftware dieser Art zeigt dem Nutzer falsche Virenmeldungen oder vermeintliche Rechnungen an. Der User soll ein vorgeschlagenes Programm herunterladen, um die Viren zu entfernen, beziehungsweise den geschuldeten Rechnungsbetrag überweisen.

RANSOMWARE

Mit einer Ransomware blockieren Cyberkriminelle den Zugang zu bestimmten Bereichen des Computers oder gar zum ganzen System und fordern Lösegeld für die Entsperrung.

Diese Liste führt nur die geläufigsten Gefahren auf, die dem heimischen PC auflauern können. Es existieren unzählige Malware-Varianten, und ständig kommen neue dazu. Eine separate Schutzsoftware ist also unerlässlich. Das Antivirenprogramm ist das Immunsystem des Computers und sollte möglichst stark und zuverlässig sein.

https://passwortcheck.datenschutz.ch

Siehe auch diverse Merkblätter zum Thema "Sicherheit" unter:

https://www.computeria-olten.ch/beratung/merkblaetter-nach-themen-a/

6. Mai 2008, Stephan Jäggi
7. Juni 2018, Manfred Peier