Neun nützliche Tipps für mehr Cybersicherheit

18. April 2019

Das Alltagsleben soll möglichst einfach und bequem sein. Oft wird deshalb die Sicherheit im Umgang mit der Informationstechnologie aus Bequemlichkeit vernachlässigt. Das ist falsch. Denn die Cyberkriminellen sind rund um die Uhr mit immer raffinierteren Methoden aktiv. Jeder erfolgreiche Cyberangriff nagt an den Nerven der Betroffenen und kann rasch ins Geld gehen. Deshalb: Die Cybersicherheit nie vernachlässigen. Hier neun nützliche Tipps dafür.

Passworte und Zwei-Faktor-Authentifizierung

Bei den Passworten wird aus Bequemlichkeit viel gesündigt. Eigentlich weiss es aber jeder: Passworte sollten über zehn Zeichen haben, aus Buchstaben, Zahlen und Sonderzeichen bestehen, zudem nicht mehrfach verwendet werden. Und: Dort wo die Zwei-Faktor-Authentifizierung mit einem Passwort oder Gesichtserkennung und zusätzlich einem über SMS oder einem Authenticator gelieferten Code möglich ist, sollte man unbedingt diese Methode wählen. Fortschrittlich ist es überdies, ein Passwortverwaltungsprogramm aus vertrauter Quelle zu nutzen, das mit einem «Masterpasswort» geschützt ist.

Keine Links oder Anhänge von irgendwie verdächtigen E-Mails öffnen

Die meisten elektronischen Schädlinge wie Viren, Würmer oder Trojanische Pferde gelangen mittels E-Mails in fremde Systeme. Deshalb gilt die Regel: Auch wenn zuweilen die Versuchung gross ist, bei allen E-Mails mit unbekannten Absendern oder bei E-Mails aus nicht hundertprozentig vertrauenswürdigen Quellen niemals Links oder Anhänge öffnen.

Mit Makros vorsichtig umgehen

Mithilfe von Makros werden häufig verwendete Aufgaben automatisiert, deren manuelle Ausführung viele Tastaturanschläge und Mausaktionen erfordert. Die seriösen Makros werden von den jeweiligen Softwareentwicklern geschrieben. Einige Makros können jedoch ein potenzielles Sicherheitsrisiko darstellen: Personen mit böswilligen Absichten können über eine Datei ein zerstörerisches Makro einschleusen, das einen Virus auf einem Computer oder im Netzwerk einer Organisation verbreitetet. Deshalb muss dafür gesorgt werden, dass böswillige Makros beispielsweise nicht mittels Office-Dokumenten eingeschleust werden können.

Verhinderung von Pishing und Betrug

Es gilt, niemandem den Benutzernamen und das dazugehörige Passwort bekanntzugeben: Kein seriöser Anbieter fragt jemals danach. Beim Onlineshopping nur bekannte Anbieter berücksichtigen, welche eine Verschlüsselung der Daten garantieren. Das ist erkennbar an der Internetadresse, die mit «https» und nicht mit «http» beginnen soll.

Vorsicht bei Tauschbörsen

Damit eine Tauschbörse im Internet funktioniert, müssen die Teilnehmer eine Software herunterladen. Achtung, diese Software kann Viren, Trojanische Pferde, Spy- und Adware oder Sicherheitslücken enthalten.

Automatische Updates nutzen

Die meisten gängigen Betriebssysteme und Computerprogramme haben heute eine automatische Updatefunktion. Diese gilt es unbedingt zu nutzen, da mit den Updates neben den Funktionsverbesserungen immer auch die neu bekannten Sicherheitslücken «gepatcht» werden.

Immer eine aktive Firewall einsetzen

Die Firewall, auf Deutsch die Brandmauer, schützt Computersysteme mittels der Überwachung aller eingehenden und ausgehenden Verbindungen. Regeln legen fest, welche Verbindungen durchgelassen werden und welche nicht. Jedes Netzwerk und jeder Rechner ist mit einer laufend geupdateten Firewall zu schützen.

Antivirensoftware laufend updaten

Die Antivirensoftware schützt die Daten vor Viren, Würmern oder Trojanischen Pferden. Es ist sicherzustellen, dass die Software laufend geupdated wird, da jeden Tag neue Viren, Würmer oder Trojanische Pferde auftauchen.

Backups machen

Trotz aller Sicherheitsmassnahmen kann nie ganz ausgeschlossen werden, dass wichtige Daten zerstört oder verloren gehen. Deshalb müssen regelmässige Backups auf Datenträgern gemacht werden, die sicher aufbewahrt werden. Dazu gehört auch eine periodische Überprüfung, ob die Sicherheitskopien vollständig und lesbar sind.