

SWISS SECURITY DAY

Fünf Schritte in Richtung Sicherheit

Am 9. März 2011 ist es wieder soweit, der 6. SwissSecurityDay findet statt. In der ganzen Schweiz werden verschiedene Anlässe und Sensibilisierungsmassnahmen durchgeführt. Das Schwerpunktthema in diesem Jahr ist der Umgang mit Social Media Plattformen wie Facebook. Fünf Schritte helfen dabei, die Computersicherheit auf einem hohen Niveau zu halten.

AUTOR: ANDREAS WISLER

Das Internet ist zu einem bedeutenden Bestandteil unseres Alltags geworden. Im Internet lesen wir die neuesten Nachrichten, rufen Fahrpläne ab, bezahlen Rechnungen oder chatten einfach mit Freunden und Bekannten.

Neben all diesen Möglichkeiten hat uns das Internet aber auch neue Gefahren gebracht. Unzählige Computerschädlinge versuchen ständig einen Weg in unseren PC zu finden,

auf welchem persönliche Daten wie Fotos, Briefe oder wichtige Dokumente gespeichert sind. Bei einem erfolgreichen Angriff können Missetäter dem Computer einen grossen Schaden zufügen, indem sie diese Daten verändern, löschen oder die darin enthaltenen Informationen dazu verwenden, um beispielsweise in Ihrem Namen oder auf Ihre Kosten im Internet einzukaufen. Die folgenden fünf Schritte helfen Ihnen, die Sicherheit Ihres Computers zu erhöhen.

Sichern

Die Datensicherung ist Ihre Lebensversicherung. Auf einem heutigen Computer sind im-

mense Datenberge gespeichert, auf welche von Zeit zu Zeit zugegriffen werden soll. Leider ist es nicht auszuschliessen, dass Daten durch Fehlmanipulationen, einen technischen Defekt oder auch durch Viren und Würmer teilweise oder komplett zerstört werden. Deshalb ist es wichtig, regelmässig die Daten auf einen externen Datenträger zu speichern. Dies kann beispielsweise auf CD/DVD, einer externen Festplatte oder auf Band erfolgen.

Schützen

Aktuelle Studien zeigen: Bewegt man sich im Internet ohne aktuellen Virens Scanner, ist der Computer innert weniger Minuten mit Schadprogrammen (Malware als Oberbegriff für Viren, Würmer, trojanische Pferde usw.) versucht. Daher ist es wichtig, ein Antivirenprogramm zu installieren und dies immer aktuell zu halten.

Überwachen

Ein Antivirenprogramm kann nicht gegen jede Malware wirken. Daher ist es notwendig, auch eine Firewall einzusetzen. Aktuelle Betriebssysteme verfügen bereits über eine entsprechende Software. In der Regel ist es nicht notwendig, eine weitere zu installieren (z.B. bei Windows Vista oder Windows 7).

ZUM AUTOR



Andreas Wisler (Tel.: 052 320 91 20,) Dipl. Ing. FH, CISSP, ISO 27001 Lead Auditor, ist Geschäftsführer der GO OUT Production GmbH, welche sich mit ganzheitlichen und produktneutralen IT-Sicherheitsüberprüfungen und -beratungen auseinandersetzt. Regelmässig veröffentlicht er einen informativen Newsletter zu aktuellen Sicherheitsthemen, der kostenlos und unverbindlich auf www.gosecurity.ch (INFONEWS) heruntergeladen werden kann. Im Rahmen des Swiss Security Days ist er für die Schulungen an der Klubschule Winterthur.

Die Aufgabe einer Firewall ist es, den Datenverkehr zu kontrollieren. Nicht benötigte «Türen» (Ports) werden durch die Firewall geschlossen und reduzieren so die Angriffsfläche des Computers.

Vorbeugen

Eine der wichtigsten Punkte ist es, die eingesetzte Software auf dem aktuellsten Stand zu halten. So zeigen beispielsweise die zahlreichen Schwachstellen im Programm Acrobat Reader, dass vorhandene Lücken sehr schnell ausgenutzt werden. Oft hilft leider hier die Antivirenlösung nicht, respektive sie ist «hintendrein». Daher gilt: halten Sie Ihre Software aktuell. Idealerweise wird dazu die automatische Aktualisierung der Programme genutzt.

Aufpassen

Der fünfte Punkt ist der gesunde Menschenverstand. Klicken Sie nicht auf jeden Link, hinterfragen Sie den Inhalt der empfangenen Email und halten Sie Ihre persönlichen

VERANSTALTUNGSHINWEIS

Informieren Sie sich direkt über die Gefahren und Möglichkeiten anlässlich des Swiss Security Days am 9. März 2011. An folgenden Orten finden dazu kostenlose Schulungen statt: Klubschule Luzern, Klubschule Winterthur, Berner Fachhochschule und Hochschule Fribourg. An verschiedenen Bahnhöfen in der Schweiz erhalten Sie Flyers und weitere Informationen. Besuchen Sie auch die Homepage www.swisssecurityday.ch oder nehmen Sie am Gewinnspiel auf Facebook teil (<http://www.facebook.com/SwissSecurityDay>).

Die im Art und weitere Punkte sind vom Bundesamt für Kommunikation BAKOM in einem abwechslungsreichen Comic zusammengefasst: «Geschichten aus dem Internet... die man selber nicht erleben möchte». Herunterladbar ist es auf der Homepage www.swisssecurityday.ch.

Daten für sich. Dies umfasst auch die Social Networks via Xing, Twitter, Facebook und Co. Teilen Sie nur «öffentliche» Sachen mit und schränken Sie die Zugriffe auf Ihre Einträge auf Ihre Freunde ein. Weiter gilt es, ein sicheres Passwort zu wählen. Dieses sollte

mindestens neun Zeichen umfassen und eine Kombination aus Zahlen, Buchstaben und Sonderzeichen sein. Um sich dies besser zu merken, kann beispielsweise ein Satz gebildet werden: «Ich besuche dieses Jahr auf jeden Fall den 6. SSD!» ergibt «IbdJajFd6.SSD!» ♦

NORMAN® Application and Device Control Sicherheitsrichtlinien durchsetzen

Behalten Sie die Oberhand

Norman Application and Device Control überwacht den unkontrollierten Einsatz mobiler Datenträger und Anwendungen im Unternehmensnetzwerk, verhindert das Einschleppen von Malware durch fremde Applikationen und Devices und unterbindet effektiv nicht autorisierte Datenspeicherungen auf Trägermedien.

Norman Application and Device bietet:

- Alle Anwendungen im Netzwerk werden erkannt
- Setzt Anwendungsrichtlinien problemlos durch
- Verbessert die Desktop- und Serververwaltung
- Lückenloses Reporting

**Jetzt
30 Tage
kostenlos
testen!**

