Special Innovation

Eine Beilage des economy-Verlages

So viel Sicherheit wie nötig

Risiken wie Datendiebstahl werden ignoriert. Dabei sind diese Gefahren genauso real wie die Möglichkeit eines Autodiebstahls. Trotzdem versperrt zwar jeder seinen Wagen, aber beim Notebook ziehen nur wenige den Schlüssel ab.

Sicherheit wird in vielen Bereichen großgeschrieben. Gegen Datendiebstahl sind aber nur die wenigsten gewappnet. Foto: Photos.com

Christian Stemberger

Internetkriminalität ist mittlerweile zu einem weltumspannenden Wirtschaftszweig geworden. Trotzdem kann auch der Laie mit ein paar simplen Maßnahmen und Regeln ein akzeptables Sicherheitsniveau erreichen. Denn wie viel in Sicherheit investiert werden sollte, hängt immer davon ab, wie schützenswert die eigenen Daten sind. Und die allererste Sicherheitsregel ist immer ein gesundes Maß Misstrauen.

Zwei globale Trends macht Thomas Blaschka, Leiter des Produktmanagements für Netzwerke und Security bei Kapsch Businesscom, derzeit aus: „Die Spam-Angriffe finden zunehmend tagesaktuell statt. Die klassischen Aufhänger wie Viagra oder Lottogewinn verlieren an Bedeutung.“ Als General Motors in groben Schwierigkeiten steckte, machte ein Mail mit dem angeblichen Selbstmord des CEO die Runde. Spam wird also immer intelligenter. Es ist nicht mehr so leicht, ihn einfach anhand der Betreffzeile zu identifizieren.

Der zweite Trend laut Blaschka ist, dass Angriffe im Cyberspace immer mehr politischen Charakter annehmen. Und die Angreifer würden keineswegs nur aus China kommen. Auch die USA sind in der Statistik ganz weit vorne. Und andere Staaten rüsten nach. Ziel dieser Attacken sind wettbewerbsrelevante Informationen, etwa Konstruktionspläne.

Schwachstellen

Zunehmend werden die sozialen Netzwerke wie etwa Facebook als Sicherheitsproblem eingestuft. Im Internet ist die Hemmschwelle, private oder berufliche Informationen gegenüber Fremden preiszugeben, niedriger als bei einem persönlichen Kontakt. Zudem erleichtert es die Suche nach potenziellen Opfern, denn sie erfolgt automatisiert.

Eine andere Sicherheitslücke tut sich bei den Smartphones auf. Apps, in der Mehrzahl sichere und sinnvolle kleine Programme, die Spiele, Zugang zu Informationsportalen oder zusätzliche Gerätefunktionen wie eine Navigationssoftware anbieten, stellen eine Möglichkeit dar, Schadsoftware auf ein Handy zu schleusen. Blaschka hält es für notwendig, dass die App-Stores von iPhone und Android nicht für jede Software offen sind: „Auch wenn Apple für die ersten Schritte in diese Richtung harsch kritisiert wird, ist dies grundsätzlich der richtige Weg.“

Wer ein Programm aus dem Internet herunterlädt, sollte immer überprüfen, ob eine unabhängige Instanz – zum Beispiel eine Fachzeitschrift – das Programm auch bewertet hat. Wer in sozialen Netzwerken unterwegs ist, sollte überlegen, wie Informationen missbraucht werden können. Kündigt man seinen Urlaub im Netz an, darf man sich auch nicht wundern, wenn die Wohnung bei der Rückkehr leer geräumt ist.

Generalschlüssel

Problematisch ist oft die Handhabung von Benutzernamen und Passwörtern, beobachtet der Sicherheitsexperte: „Wenn man seinen wirklichen Namen oder die E-Mail-Adresse als Benutzername verwendet und dazu immer dasselbe Passwort, dann ist das ein Generalschlüssel.“ Zumindest beim Onlinebanking oder Ebay-Account sollte man etwas vorsichtiger sein. Blaschka fordert nichts Unmögliches: „Wer sich kein Passwort merken kann, darf es auch aufschreiben.“ Nur zu offensichtlich dürfe es nicht sein, mit ein wenig Kreativität finde sich ein unverdächtiger Ort wie etwa eine Notiz im Kalender – und „Passwort“ oder „Banking“ solle tunlichst nicht dabeistehen.

Das Virenschutzprogramm auf dem PC, im Privatbereich kann es durchaus auch eine Freeware sein, ist Pflicht. Und alle zwei Wochen sollte das ganze System gescannt werden. Wobei Blaschka auch hier Realist bleibt: „Einmal im Monat ist besser als gar nicht.“ Großen Nachholbedarf ortet er beim Verschlüsseln mobiler Endgeräte wie Laptops oder PDA: „Das sollte so selbstverständlich wie das Absperren des Autos sein.“

Ebenfalls im Argen liegt die Verschlüsselung des Datentransfers von mobilen Geräten: „Smartphones und Laptops sind oft vollkommen ungeschützt. Jedes E-Mail kann mitgelesen werden.“ Hier scheitert es an einer benutzerfreundlichen Lösung. Die soll aber, so der Kapsch-Experte, innerhalb der nächsten 18 Monate für den Enterprise-Markt zur Verfügung stehen.

Und wenn einmal die Privat-User ihre Daten nicht mehr lokal, sondern bei einem Provider in der „Wolke“ speichern werden, dann werden auch sie über eine End-to-end-Verschlüsselung auf sie zugreifen können.

www.kapsch.net