

“Wie hoch ist mein Risiko?” – Praxis-Leitfaden für den engagierten Webnutzer

Gastbeitrag von Frank Herberg

Wie erlebt eigentlich ein ausgewiesener Sicherheits-Experte seine eigenen Aktivitäten im Social Web? Wie schützt er sich? Was traut er sich? Was lässt er lieber sein? Und was empfiehlt er anderen? All das habe ich mich schon öfter gefragt, wenn ich mit Frank Herberg beispielsweise via Facebook kommuniziert habe. Kürzlich wollte ich von ihm wissen, wie sicher eigentlich mein Dropbox-Account ist. Dabei entstand die Idee zu diesem Gastbeitrag. Mehr Informationen über den IT-Spezialisten und weiterführende Links finden Sie am Ende dieses Ratgebers. (Kerstin Hoffmann)



Webworker verbringen jeden Tag viele Stunden online am Computer und nutzen dabei eine ständig steigende Zahl an Diensten. Begeisterung über die dazugewonnene Funktionalität oder die neue Bequemlichkeit lässt dabei oft darüber hinwegsehen, welches Risiko vielleicht ebenfalls damit verbunden ist. Außerdem werden Best-Practices, die jeder von uns schon mal gehört hat, in der Praxis oft vernachlässigt.

Wenn Ihre letzte Bestandsaufnahme in Sachen Online-Sicherheit schon eine Weile her ist, hilft Ihnen der folgende Checkup, Ihr persönliches Risiko einzuschätzen. Zudem erfahren Sie, welche Maßnahmen helfen, um Ihren Web-Arbeitsplatz auch hinsichtlich Sicherheit up-to-date zu halten – und warum das Ihren nächsten Urlaub retten kann.

Halten Sie Ihre Software aktuell?

Früher hatte man oft Hemmungen, etwas an seinem PC zu verändern, wenn gerade mal alles stabil lief. Heute dienen Updates jedoch oft dazu, Sicherheitslücken zu schliessen, die Ihr System sonst angreifbar machen. Angriffe auf Schwachstellen werden heute meist schon kurz nach Bekanntwerden der Sicherheitslücke ausgeführt.

Denken Sie dabei bitte nicht, dass es ein Angreifer auf Sie persönlich abgesehen haben muss. Diese Angriffe auf Schwachstellen werden heute großflächig und automatisiert durchgeführt. Danach tut ihr Computer vielleicht Dinge, die Sie nicht möchten – und vielleicht auch lange nicht bemerken.

Folgende Software sollten Sie möglichst zeitnah und am besten automatisiert mit Sicherheits-Updates versorgen:

- Betriebssystem
- Webbrowser und Plug-ins
- Software wie Flashplayer, Acrobat-Reader, etc.
- Virens Scanner und sonstige Sicherheits-Tools

Größere Updates, die dazu dienen, die Funktionalität zu erweitern, wollen Sie vielleicht manuell anstossen. Denn wenn gerade die Deadline für die Abgabe eines Angebots oder Arbeitsergebnisses kurz bevor steht, kommen solche Änderungen am System eher ungelegen. (Dazu muss der Softwarehersteller natürlich auch zwischen Sicherheits- und anderen Updates unterscheiden.)

Können Sie Ihrem Computer noch vertrauen?

De facto vertrauen Sie jeder Software, die Sie installieren, dass Sie nur das tut, was sie vorgibt. Dies gilt auch und gerade für die vielen Add-ons, Plug-ins und sonstigen Helferlein, die sich mit der Zeit auf jedem Computer ansammeln. Natürlich 'lebt' Ihr Arbeitsplatz von einer guten Auswahl an Software, die Ihnen das Leben leichter macht. Aber mit einer wachsenden Zahl an Programmen und Progrämmchen wird er auch tendenziell instabiler, langsamer und – unsicherer!

Für jeden mittelmäßig begabten Computerfreak ist es ein leichtes, gängige Softwarepakete um eine Malware – ein Stück schädliche Software – zu erweitern. Das liest dann beispielsweise Ihre Kennworteingaben mit und sendet sie an jemanden, der sich dafür interessiert. Im Internet gibt's fertige Kits, um sowas zu bauen.

Besorgen Sie sich deshalb Ihre Software immer aus vertrauenswürdigen Quellen. Installieren Sie nichts aus E-Mails oder von irgendwelchen Internetseiten, die Sie nicht einschätzen können. Besser geeignet sind

- Download-Seiten vom Hersteller oder Softwareprojekt
- seriöse Software-Archive, wie es sie bei Heise, Chip, ZDnet oder sourceforge gibt.

Achten Sie auch darauf, was Ihnen wirklich nützt. Und deinstallieren Sie von Zeit zu Zeit wieder, was Sie nicht brauchen.

Unterwegs mit dem Laptop? Folgendes gilt es zu beachten

Ein Laptop, den Sie mobil einsetzen, ist naturgemäss deutlich stärkeren Auflösungskräften ausgesetzt, als der Desktop-PC, der warm und trocken auf oder unter dem heimischen Schreibtisch steht. Alleine am Flughafen Frankfurt gehen wöchentlich etwa 300 Laptops verloren. Aber auch ein Totalschaden durch Schwerkrafteinfluss oder verschüttete Getränke ist nicht selten.

Wenn sowas passiert, sollten Sie zum einen auf eine aktuelle Datensicherung zurückgreifen können und zum anderen sicher sein, dass der Dieb mit den auf dem Gerät gespeicherten Informationen keinen Schaden anrichten kann.

Was haben Sie alles auf Ihrem Laptop gespeichert?

Auch wenn Sie vielleicht keine Geschäftsgeheimnisse oder Kundeninterna auf der Festplatte haben: Der Zugriff auf all Ihre Dokumente und Zugangsdaten lässt sich gezielt missbrauchen. Allein Ihr Mailaccount öffnet Tür und Tor für das Zurücksetzen aller möglichen Kennwörter und Online-Zugänge.

Denken Sie einmal ein paar Minuten drüber nach, was in Ihrem persönlichen Fall damit alles verbunden sein könnte. Dies wieder rechtzeitig einzufangen, wird viel Zeit und Nerven kosten. Wer gerade auf dem Weg in den Urlaub war, wird sich vielleicht sogar entschließen, diesen abubrechen.

Passwörter von BIOS und Betriebssystem bieten nur Schutz für die ersten sagen wir fünf Minuten. Ab Minute sechs ist dann entscheidend, ob Sie Ihre Daten verschlüsselt haben. Und das ist weder 'nerdy' noch schwer. Man muss es nur tun.

Nutzen Sie Masterpasswort und Passwort-Safe!

Ihre gespeicherten Passwörter können Sie in vielen Programmen (z.B. Firefox oder Thunderbird) mit einem sogenannten Masterpasswort versehen. Dieses müssen Sie einmalig eingeben, wenn Sie das Programm benutzen, es ver- und entschlüsselt dann alle Ihre gespeicherten Passwörter. Zudem gibt es sogenannte Passwort-Safes, die diesen Job machen.

Das Schöne dabei ist, dass Sie nun all Ihre Passwörter für die verschiedensten Onlinezwecke unterschiedlich halten und kompliziert genug machen können – beides entscheidende Faktoren für deren Sicherheit.

Persönliche Daten? Kundendaten? Verschlüsseln!

Der nächste Schritt ist das Verschlüsseln Ihrer Daten. Während die Foto- und Musiksammlung vielleicht unbedenklich ist, gilt das bei persönlichen Dokumenten, Verträgen und Kundendaten nicht.

Eine anerkannt sichere Software zum Verschlüsseln ist TrueCrypt. Sie ist für Windows, Mac und Linux kostenlos verfügbar. Damit können Sie auch ohne Kryptographie-Studium nach kurzer Zeit Dateicontainer anlegen, in denen Sie Ihre sensiblen Daten sicher ablegen. Ausserdem können Sie mobile Datenspeicher (Backup-Festplatte, USB-Stick) damit einfach verschlüsseln. Beruhigend auch, wenn der USB-Stick mal wieder unauffindbar ist.

Wer seinen Computer schon einmal spontan zur Reparatur bringen musste, wird auch ohne Diebstahl schnell von dem Nutzen überzeugt sein. Und wenn die Hardware ihre zweite Lebenshälfte im Second-Hand-Markt antritt oder auf dem Müll landet, sind Ihre Daten so immer noch sicher. Löschen und Formatieren reichen hier ja bekannterweise nicht.

Im@inter09@imCiF! – einfach komplizierte Passwörter merken

Wichtig ist, dass Sie das Masterpasswort oder die 'Keyphrase' für TrueCrypt wirklich sicher wählen. Das bedeutet *mehr* als 8 Zeichen *und* schwer zu erraten oder auszuprobieren. Denn natürlich kann man die Verschlüsselung angreifen (Tools dazu gibt es frei im Netz). Zu einfache Passwörter sind sehr schnell geknackt.

- Am besten nehmen Sie sich einen individuellen Satz, den Sie sich gut merken können, wie "Im Winter 09 war ich mit Chris in Florida!"
- Leiten Sie daraus Ihre Keyphrase ab, z.B. "ImWinter09wimCiF!"
- Wer will, kann jetzt noch einen Buchstaben durch ein Sonderzeichen ersetzen, z.B. das '@', das auf der Tastatur über dem 'W' liegt: " Im@inter09@imCiF!"

Voilà!

Backup – machen!

Wer bei einem 'plötzlichen' Defekt, Diebstahl, Löschen – versehentlich durch den Benutzer oder absichtlich durch einen Virus – entspannt bleiben will, braucht eine aktuelle Datensicherung. Leider ist diese trotz besseren Wissens oft nicht da, wenn man sie braucht. Ein paar Praxis-Tipps:

- Daten, die sich nicht mehr verändern (z.B. Urlaubsfotos), können Sie einmalig auf einer externen Festplatte sichern.
- Daten, die sich häufig ändern, (z.B. Ihre aktuelle Arbeit) von denen Sie ggf. auch auf mehrere Versionen zurückgreifen können möchten, könnten Sie z.B. online sichern.
- Besonders schützenswerte Daten (Arztrechnungen, Verträge, die PIN-Sammlung, etc.), sollten Sie immer verschlüsseln, egal wo die Sicherung gespeichert wird.
- Denken Sie auch an Ihre Bookmarks (Favoriten), diese lassen sich in eine Datei exportieren – und an das lokal gespeicherte Mail-Archiv mitsamt der Adressen.

Natürlich gibt es eine Vielzahl von Backup-Tools, mit denen Sie sich einen Teil der regelmässigen Arbeit abnehmen lassen können. Bedenken Sie dabei zwei Punkte:

- Vergewissern Sie sich, dass das Tool richtig sichert: Testen Sie das Zurücksichern.
- Sorgen Sie dafür, dass das Tool im Fall eines Festplattencrashes noch (in der richtigen Version) verfügbar ist.

Was sollten Sie bei Online-Speichern wie Dropbox, Skydrive und Co. beachten?

Ungemein praktisch ist es, wenn man seine Daten irgendwo auf einem Server im Internet ablegen und von überall darauf zugreifen kann. Bedenken Sie dabei: Daten sind der Rohstoff des Informationszeitalters. Alles, was Sie ins Netz hochladen, ist im Zweifel nicht mehr kontrollierbar, kann nicht mehr gelöscht werden und wird unter Umständen personenbezogen analysiert und weiterverwertet.

Schauen Sie sich deshalb die Online-Dienste, die Sie benutzen möchten, genau an. Hierzu lohnt sich ein Blick in die AGB. Ausserdem sollte man sich über die wirkliche Sicherheit des Anbieters unabhängig informieren.

Beispiel Dropbox: Ein Zitat aus den AGB (Privacy Policy): "*Dropbox may sell [...] your Personal Information[...]*". Uups. – Ausserdem entlarvt eine technische Sicherheitsbetrachtung von Dropbox: Ihre Daten werden zwar verschlüsselt – aber dieser Schlüssel ist Dropbox bekannt. Dropbox hat also Zugriff auf all ihre Daten.

Aber auch hier naht Hilfe: Sie können TrueCrypt mit Dropbox kombinieren. Damit haben nur Sie den Schlüssel für Ihre Daten.

Ein wenig Privatsphäre im Netz schaffen

Wenn Sie sich heute im Internet bewegen, schauen Ihnen dabei einige sehr genau zu. Das Erstellen von detaillierten Nutzerprofilen ist ein großes Geschäft. Facebooks Social Plugins, Google Analytics und der Werbeverbund NAI sind bekannte Beispiele. Wer kein Interesse daran hat, dass ihm Google und Co. überall hin folgen, kann einfache Gegenmaßnahmen ergreifen. Das Versetzen des Browsers in den 'privaten Modus' und der Einsatz von sogenannten Werbeblockern wie 'AdBlock Plus' sind zwei gute Beispiele.

Wenn Sie mehr darüber erfahren wollen, wie Sie Ihre Privatsphäre im Netz ein Stück weit schützen können, empfehle ich Ihnen den kostenlosen Internet-Privacy-Workshop ab kommender Woche [in meinem Blog](#).

Dieses Thema betrifft viele von uns nicht nur aus Nutzersicht. Auch als Webseitenbetreiber sollten Sie darüber Bescheid wissen, wie die Technologien, die Sie in Ihre Seite einbinden, Ihre Webseitenbesucher ausspionieren. Je nach Branche kann der Image-Schaden beim Einsatz solcher Möglichkeiten den Nutzen weit übersteigen.

Worauf Sie verzichten können

Delegieren Sie Ihre Sicherheit nicht an eine 'Security-Suite'. Diese beinhalten in der Regel alles mögliche von der Personal Firewall, über den Virenschanner bis zum Verschlüsselungstool und dem Adblocker. Oft wird hier dem verunsicherten Benutzer gegen Geld ein Rundumschutz versprochen, bei dem er sich um nichts mehr selber kümmern muss. In kritischen Tests schneiden solche oft sehr umfangreichen Suites regelmässig mangelhaft ab, weil sie neben Stärken in einem Bereich woanders gravierende Schwächen aufweisen. Viel besser ist es, für jede Aufgabe gezielt und unabhängig das Tool einzusetzen, das für den jeweiligen Bereich wirklich geeignet ist.

Fazit

Das Internet ist lange seinen Kinderschuhen entwachsen. Dies eröffnet uns einerseits viele faszinierende Möglichkeiten. Auf der anderen Seite sind wir gefordert, ein solides Grundverständnis für die verbundenen Risiken zu entwickeln und up-to-date zu halten. Mit dem Wissen um die geeigneten Verfahren und Tools kann jeder ohne allzu grossen Aufwand dafür sorgen, dass er auf der sicheren Seite ist.

Links zu den genannten Tools, Anleitungen für deren Einsatz und weiterführende Informationen gibt es [hier](#).

-

Frank Herberg, Jahrgang 1969, lebt in Zürich und ist Informationstechnologie-Profi aus Leidenschaft. In seinen Spezialgebieten IT-Infrastruktur, Netzwerke und Security verfolgt er aktuelle Entwicklungen seit mehr als 15 Jahren. Sein Know-how setzte er in den vergangenen Jahren als Technologie-Berater und Projekt-Manager in verschiedenen internationalen IT-Projekten in die Praxis um. Zur Zeit genießt er ein Sabbatical. In seinem Techblog gibt er Anwendertipps und schreibt über Themen wie neue Technologien oder Internetsicherheit.

© Kerstin Hoffmann, <http://www.pr-doktor.de>
Weitergabe ausschließlich komplett mit Quellenangabe. Jegliche Veröffentlichung und Verwendung nur mit Genehmigung. Foto: © Klaus Eck