Schützen - aber wie?

Ohne Frage - für Ihre Sicherheit müssen Sie etwas tun. Aber der Aufwand lohnt sich. Denn wer rechtzeitig vorsorgt und seine Daten schützt (und regelmäßig sichert) reduziert das Schadensrisiko erheblich. Diese Vorsorge kann Ihnen Zeit, Geld und Nerven ersparen. Die bräuchten Sie nämlich ganz sicher, wenn der Schaden erst einmal da ist. Mehr Informationen zum richtigen Umgang mit Passwörtern und zur Datenverschlüsselung finden Sie auf den folgenden Seiten.

Wieviel Aufwand Sie betreiben müssen, hängt - wie immer - von Ihren persönlichen Anforderungen ab. Und selbst wer jetzt denkt: "Welche Informationen sollen auf meinem PC schon zu holen sein..." - auch der ist hier genau richtig. Denn auch für den gilt: Fast jeder besitzt Informationen, die in die falschen Hände gelangen könnten.

Um das zu verhindern kommt es besonders auf zwei Dinge an: Erstens sollten Sie Ihren eigenen PC (bestimmte Anwendungen und ausgewählte Informationen) mittels Passwörter schützen und zweitens Daten, die übertragen werden müssen, verschlüsseln. Mehr Informationen zum richtigen Umgang mit Passwörtern und zur Datenverschlüsselung finden Sie auf den folgenden Seiten. Los geht's aber zunächst mit der Frage "Wer braucht welchen Schutz?" und einem Überblick über die wichtigsten Schutzmaßnahmen.

Wer braucht welchen Schutz?

Wieviel Aufwand Sie zum Schutz Ihres PCs - und somit natürlich auch zum Schutz Ihrer Privatsphäre - betreiben müssen, hängt in erster Linie von Ihren persönlichen Anforderungen ab. Es gibt jedoch Schutzmaßnahmen, die Sie in jedem Fall treffen sollten.

Die zehn wichtigsten Tipps, die Internetnutzer für ein ungetrübtes Surf-Vergnügen immer beherzigen sollten, haben wir zudem in einer Übersicht zusammengestellt.

Basisschutz leicht gemacht!

1. Installieren Sie ein Virenschutzprogramm und ein Anti-Spyware-Programm und halten Sie diese immer auf dem aktuellen Stand.
2. Setzen Sie eine Personal Firewall ein und aktualisieren Sie diese regelmäßig. Sie schützt bei richtiger Konfiguration vor Angriffen aus dem Internet und verhindert zudem bei einer Infektion des PCs mit einem Computerschädling, dass ausspionierte Daten an einen Angreifer übersendet werden können.
3. Achten Sie darauf, ob es Sicherheitsupdates für Ihr Betriebssystem und sonstige von Ihnen installierte Software gibt und führen Sie diese durch.
4. Arbeiten Sie nach Möglichkeit nicht als Administrator an Ihrem PC, denn so können Schadprogramme noch mehr Unheil anrichten. Richten Sie für alle Nutzer eines PCs unterschiedliche Benutzerkonten ein. Vergeben Sie für diese

Konten nur die Berechtigungen, die der jeweilige Nutzer für seine Arbeit braucht. So werden auch private Dateien vor dem Zugriff Anderer geschützt.

5. Gehen Sie sorgfältig mit Ihren Zugangsdaten um: Halten Sie Kennwörter und Benutzernamen sowie Zugangscodes für Dienste (z. B. beim Online-Banking) unter Verschluss. Wechseln Sie Passwörter in regelmäßigen Abständen.
6. Seien Sie vorsichtig beim Öffnen von E-Mail-Anhängen. Schadprogramme werden oft über Dateianhänge in E-Mails verbreitet. Im Zweifelsfall fragen Sie vorsichtshalber beim Absender nach, ob der Anhang tatsächlich von ihm stammt.
7. Seien Sie vorsichtig bei Downloads von Webseiten. Vergewissern Sie sich vor dem Download von Programmen aus dem Internet, ob die Quelle vertrauenswürdig ist und bringen Sie Ihr Virenschutzprogramm auf den aktuellsten Stand.
8. Seien Sie zurückhaltend mit der Weitergabe persönlicher Informationen. Online-Betrüger steigern ihre Erfolgsraten, indem sie individuell auf ihre Opfer zugehen: Zuvor ausspionierte Daten, wie etwa Surfgewohnheiten oder Namen aus dem persönlichen Umfeld, werden dazu verwandt Vertrauen zu erwecken.
9. Nutzen Sie Übertragungstechnologien wie Voice over IP (VoIP) oder Wireless LAN (WLAN), dann achten Sie besonders auf eine Verschlüsselung Ihrer Kommunikation, damit die Übertragung Ihrer Daten nicht von Dritten mitgelesen bzw. Gespräche nicht abgehört werden können.
10. Kommt es trotz aller Schutzmaßnahmen zu einer Infektion des PCs mit einem Schädling, können wichtige Daten verloren gehen. Um den Schaden möglichst gering zu halten, sollten Sie regelmäßig Sicherungskopien Ihrer Dateien auf CD-ROM/DVD oder externen Festplatten erstellen.

Passwörter

Wer die Wahl hat, hat die Qual - heißt es. Besonders bei **der Wahl der richtigen Passwörter** tun sich viele PC-Nutzer schwer. Um dem zu entgehen, kommt es nicht selten vor, dass jemand ein Passwort für zehn verschiedene Programme bzw. Zugänge hat. Wen wundert's da, dass schlecht gewählte Passwörter auf der Hitliste besonders häufiger IT-Sicherheitsdefizite ganz weit oben stehen. Hacker freut das natürlich. Sie haben Werkzeuge, die vollautomatisch alle möglichen Zeichenkombinationen ausprobieren oder ganze Wörterbücher einschließlich gängiger Kombinationen aus Worten und angefügten Zahlen testen. Um das zu verhindern, sollte ein Passwort bestimmte Qualitätsanforderungen erfüllen.

Hinzu kommt, dass Passwörter nicht nur zum Schutz von vertraulichen Daten dienen. Ein Beispiel: Inzwischen ist es üblich, dass man sich bei unterschiedlichsten Anbietern im Internet ein Konto oder einen Zugang (Account) anlegen kann. Die Anmeldung an diesem Account wird mit einem Passwort geschützt. Was könnte passieren, wenn sich jemand unter Ihrem Namen dort anmeldet? Wer möchte schon gerne, dass Fremde unter dem eigenen Namen E-Mails verschicken oder teure Waren im Internet ersteigern können?

Deshalb: Orientieren Sie sich an den folgenden Empfehlungen – und schon tun Sie etwas mehr für Ihre Sicherheit.

Tipps

Ein gutes Passwort

... sieht so aus: Es sollte mindestens acht Zeichen lang sein. Tabu sind allerdings Namen von Familienmitgliedern, des Haustieres, des besten Freundes, des Lieblingsstars usw. Und wenn möglich sollte es nicht in Wörterbüchern vorkommen. Zusätzlich sollte es auch Sonderzeichen (?!%.....) und Ziffern enthalten. Dabei sollten allzu gängige Varianten vermieden werden, also nicht 1234abcd usw. Einfache Ziffern am Ende des Passwortes anhängen oder eines der üblichen Sonderzeichen $, !, ?, #, am Anfang oder Ende eines ansonsten simplen Passwortes ist auch nicht empfehlenswert.

Aber wie merkt man sich ein solches Passwort? Auch dafür gibt es Tricks. Eine beliebte Methode funktioniert so: Man denkt sich einen Satz aus und benutzt von jedem Wort nur den 1. Buchstaben (oder nur den 2. oder letzten, etc.). Anschließend verwandelt man bestimmte Buchstaben in Zahlen oder Sonderzeichen. Hier ein Beispiel: "Morgens stehe ich auf und putze meine Zähne." Nur die 1. Buchstaben: "MsiaupmZ". "i" sieht aus wie "1", "m" ist eine liegende "3": "Ms1aup3Z". Auf diese Weise hat man sich eine gute "Eselsbrücke" gebaut. Natürlich gibt es viele andere Tricks und Methoden, die genauso gut funktionieren. Manchmal kann es trotz dieser Merkhilfen sinnvoll sein, sich Passwörter aufzuschreiben. Dazu steht bei Punkt 3 mehr.

Passwörter regelmäßig ändern

Jedes Passwort sollte in regelmäßigen Zeitabständen geändert werden. Viele Programme erinnern Sie automatisch daran, wenn Sie das Passwort z.B. schon ein halbes Jahr benutzen. Diese Aufforderung nicht gleich wegklicken – sondern ihr am besten gleich

nachkommen! Natürlich ist es da schwer, sich alle Passwörter zu merken. Womit wir beim nächsten Punkt sind.

Passwörter nicht notieren

Auch wenn es bei selten genutzen Zugangsdaten schwerfällt – grundsätzlich sollten Sie sich Passwörter nicht aufschreiben.

Keine einheitlichen Passwörter verwenden

Problematisch ist die Gewohnheit, einheitliche Passwörter für viele verschiedene Zwecke bzw. Zugänge (Accounts) zu verwenden. Denn gerät das Passwort einer einzelnen Anwendung in falsche Hände, so hat der Angreifer freie Bahn für Ihre übrigen Anwendungen. Das können z. B. die Mailbox oder alle Informationen auf dem PC sein.

Voreingestellte Passwörter ändern

Bei vielen Softwareprodukten werden bei der Installation (bzw. im Auslieferungszustand) in den Accounts leere Passwörter oder allgemein bekannte Passwörter verwendet. Hacker wissen das: Bei einem Angriff probieren sie zunächst aus, ob vergessen wurde, diese Accounts mit neuen Passwörtern zu versehen. Deshalb ist es ratsam, in den Handbüchern nachzulesen, ob solche Accounts vorhanden sind und wenn ja, diese unbedingt mit individuellen Passwörtern abzusichern.

Bildschirmschoner mit Kennwort sichern

Bei den gängigen Betriebssystemen haben Sie die Möglichkeit, Tastatur und Bildschirm nach einer gewissen Wartezeit zu sperren. Die Entsperrung erfolgt erst nach Eingabe eines korrekten Passwortes. Diese Möglichkeit gibt es nicht umsonst. Deshalb: Nutzen Sie sie! Ohne Passwortsicherung können unbefugte Dritte sonst bei vorübergehender Abwesenheit des rechtmäßigen Benutzers Zugang zu dessen PC erlangen. Natürlich ist es ziemlich störend, wenn die Sperre schon nach weniger Zeit erfolgt. Unsere Empfehlung: 5 Minuten nach der letzten Benutzereingabe. Zusätzlich gibt es die Möglichkeit, die Sperre im Bedarfsfall auch sofort zu aktivieren (z.B. bei einigen Windows-Betriebssystemen: Strg+Alt+Entf drücken).

Datenverschlüsselung

Haben Sie sich schon einmal Gedanken darüber gemacht, ob Sie bei Ihren **Telefongesprächen, E-Mails oder besuchten Internetseiten ausspioniert werden**? So unwahrscheinlich ist das nicht. Allerdings ist es auch nicht unmöglich, sich davor zu schützen. Eine Möglichkeit ist, die **Nachrichten zu verschlüsseln**. Da gibt es **symmetrische** und **asymmetrische** Verfahren, **digitale Signaturen** und die **PKI**.
Doch bevor wir dazu kommen, geht es um die Frage: Warum wird überhaupt verschlüsselt?

Daten werden verschlüsselt, um sie zu schützen. Die Verschlüsselung im Internet dient **drei Zielen**:

- Schutz der Vertraulichkeit: Die Nachricht darf nur für den lesbar sein, für den sie bestimmt ist.

- Schutz der Authentizität: Die Echtheit des Absenders soll gewahrt sein. Ist der Absender wirklich die Person, die als Absender angeben wird?
- Schutz der Integrität: Die Nachricht darf auf dem Weg vom Absender zum Empfänger nicht verändert werden.

Verschlüsselungsverfahren

Die Verschlüsselungsverfahren lassen sich danach unterscheiden, wie ein Text verschlüsselt und wieder entschlüsselt werden kann.

- Symmetrische Verschlüsselung
- Asymmetrische Verschlüsselung
- PKI und Digitale Signatur

Welche Verfahren gibt es?
Symmetrische Verschlüsselung:

Stellen Sie sich vor, Sie wären ein römischer Feldherr und hätten ziemlichen Ärger mit den Germanen. Um diesen eine gehörige Lektion zu erteilen, wollen Sie Ihren Truppen einen geheimen Angriffsbefehl per Boten zukommen lassen. Weil Sie aber befürchten, dass der Bote unterwegs in Feindeshand gerät, chiffrieren Sie die Nachricht.

Der Text sieht dann so aus:

"DQJULIILPPRUJHQJUDXHQ"

Tatsächlich fangen die Germanen den Boten und versuchen nun eifrig, den Inhalt zu entziffern. Nach ein wenig Knobeln erhalten Sie den Text in Klarschrift. Versuchen Sie es doch auch einmal!

Jeder Buchstabe wurde durch seinen dritten rechten Nachbarn im Alphabet ersetzt.

```
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
```

Der verschlüsselte Text heißt in Klarschrift also: "Angriff im Morgengrauen".

Dieses Verfahren wurde damals tatsächlich von den Römern angewandt. Benannt ist es nach seinem Erfinder Caesar. So richtig schwierig ist es aber nicht, oder?

Es gibt aber auch andere Mechanismen um Nachrichten so zu chiffrieren. Die können nur sehr schwer oder überhaupt nicht geknackt werden. Das glauben Sie nicht? Versuchen Sie jetzt einmal diese Botschaft aufzudecken!

"XZKYDXOWFVCUCTFSJRJQLPOODNBMKLDKOJXIRHBGKF"

Die Verfahrensregel lautet hier: Jeden Buchstaben durch seinen dritten linken Nachbarn im Alphabet ersetzen und dazwischen jeweils einen Buchstaben zusätzlich als "Blender" einfügen, wobei mit Z beginnend absteigend das Alphabet durchgegangen wird. Das war schon knifflig, und man könnte sich noch viel schwierigere Verfahren ausdenken. Die Botschaft war übrigens die gleiche.

In einem Computer funktioniert das ganze auch, allerdings versteht dieser **nur Nullen und Einsen**. Anstelle des Textes tritt nun eine Folge der beiden Zahlen. Diese könnte etwa so aussehen: 010101001011001001

Um die Zahlenfolge zu chiffrieren, kann man eine Rechenregeln anwenden, wie z.B. eine Additionsregel, die so heißen kann: 0+0=0; 1+0=1; 0+1=1 und 1+1=0. Anstelle von Buchstaben werden hier jetzt Zahlen vertauscht. Allerdings haben wir jetzt zwar eine Zahlenreihe und ein Rechenverfahren, aber mit was soll denn bitteschön addiert werden?

Sie ahnen es vielleicht bereits: Mit einem Schlüssel, der selbst wieder aus einer Reihe von Nullen und Einsen besteht. Nehmen wir einmal an, der sieht so aus:

001101000100010011

Also addieren wir diese beiden Zahlenfolgen einmal miteinander:

	0101010010110010 01	Nachricht
+	0011010001000100 11	Schlüssel
=	0110000011110110 10	Chiffrat

Sie sehen, der Schlüssel ist genauso lang wie die Originalnachricht. Es gibt also sehr viele Möglichkeiten, wie dieser aussieht. Je länger der Schlüssel ist, desto mehr Variationen gibt es, und um so schwieriger ist es, die geheimen Nachrichten zu dechiffrieren.

Bei einem solchen schlüsselabhängigen Verfahren kann übrigens die Rechenregel jedem bekannt sein, solange nur der Schlüssel geheim bleibt.

Um das Chiffrat wieder in die Ursprungsnachricht zurückzuverwandeln, müssen Sie entweder mit dem Schlüssel subtrahieren oder die Addition einfach noch einmal durchführen.

Sender und Empfänger müssen deshalb über den gleichen Schlüssel verfügen. Schwierig ist dabei, den Schlüssel so auszutauschen, ohne dass ihn ein unbefugter Dritter dabei ausspionieren kann.

Ein anderes Problem der symmetrischen Verschlüsselung tritt auf, wenn sehr viele Leute miteinander kommunizieren wollen. Nehmen wir an, dass 12 Leute verschlüsselt Botschaften austauschen möchten. Weil aber manchmal zwei Leute Geheimnisse untereinander haben, von denen niemand sonst erfahren soll, wollen sie verhindern, dass die jeweils übrigen 10 mitlesen können. Wie viele Schlüssel werden hier also insgesamt benötigt?

Der erste benötigt zunächst 11 Schlüssel. Für sich selbst braucht er zwar keinen, aber für jeden anderen jeweils einen. Der zweite benötigt zwar auch 11 Schlüssel, aber einer davon wurde schon bei dem ersten mitgerechnet. Rechnet man so weiter ergibt sich: 11 + 10 + 9 + 8 + 7 + 6 + 5 + 4 + 3 + 2 + 1 = 66. Bei 50 Personen sind es übrigens 1225, bei 1000 Leuten sogar fast 500.000 verschiedene Schlüssel. Nicht auszudenken, wenn das alle Leute so machen wollen!

Diese beiden Probleme der symmetrischen Verschlüsselung werden mit so genannten asymmetrischen Verfahren gelöst.

Asymmetrische Verschlüsselung:

Bei der asymmetrischen Verschlüsselung **gibt es immer zwei sich ergänzende Schlüssel**. Ein Schlüssel - der **Public Key** - für das Verschlüsseln einer Nachricht, ein anderer - der **Private Key** - für das Entschlüsseln. Beide Schlüssel zusammen bilden ein Schlüsselpaar.

Das Besondere an der Sache ist, dass aus dem einem Schlüssel der dazugehörige zweite Schlüssel nicht so leicht erraten oder berechnet werden kann. Dadurch kann man einen Schlüssel des Schlüsselpaares für jedermann öffentlich zugänglich machen. Daher auch die Bezeichnung Public Key.

Stellen Sie sich am besten einen Tresor mit Schnappschloss vor. Sie können etwas einschließen, weil der Tresor sich automatisch schließt, wenn die Tür ins Schloss fällt. Zum Öffnen benötigen Sie allerdings einen Schlüssel. Wie bei dem Tresor kann also jeder mit dem Public Key etwas einschließen. Weil aber nur der Empfänger über den geheimen, den Private Key verfügt, kann nur er die Nachricht entziffern oder etwas aus dem Tresor holen.

Die asymmetrische Verschlüsselung beruht auf mathematischen Verfahren, die in einer Richtung einfach aber in der anderen Richtung schwierig durchzuführen sind. Multiplizieren ist so ein Beispiel:

Jeder kann einfach zwei Zahlen multiplizieren, zum Beispiel:
3 121 163 * 4 811 953 = 15 018 889 661 339
Zahlen in Faktoren zu zerlegen, ist dagegen sehr mühselig: Hat man erst einmal das Produkt, ist es sehr schwierig herauszufinden, aus welchen Faktoren dieses ursprünglich gebildet wurde. Versuchen Sie doch einmal (wenn Sie viel, viel Zeit haben) herauszufinden, aus welchen Faktoren die Zahl 11 099 399 206 043 besteht.

Das Problem mit dem Schlüsselaustausch ist daher elegant gelöst: Der öffentliche Teil kann jedem zugänglich gemacht werden, ohne dass die Sicherheit darunter leiden würde. Man benötigt ja immer noch den geheimen Schlüssel. Ein weiterer Vorteil des Verfahrens ist, dass sehr viel weniger Schlüssel benötigt werden als beim symmetrischen Verfahren. Denn jeder benötigt ja nur ein Schlüsselpaar.

Aber auch asymmetrische Verschlüsselungsverfahren haben **Schattenseiten**:

- Erstens sind asymmetrische Verfahren, im Vergleich zu symmetrischen Verfahren, sehr rechenaufwändig. Um kurze Nachrichten zu verschlüsseln, benötigt der Computer viel Zeit. Deshalb bedient man sich eines Tricks: Mit dem langsamen, asymmetrischen Verfahren werden nur die Schlüssel für ein schnelles symmetrisches Verfahren sicher und unkompliziert ausgetauscht. Die weitere Kommunikation erfolgt dann über die schnellere symmetrische Verschlüsselung. Weil asymmetrische Verfahren dafür genutzt werden, die Schlüssel eines symmetrischen Verfahrens zu verschlüsseln, nennt man es hybride - also kombinierte - Verschlüsselung.

- Zweitens kann keiner so leicht rauskriegen, ob der verwendete Public Key auch wirklich demjenigen gehört, dem man die verschlüsselte Nachricht schicken will. Im Internet ist es leicht sich für jemanden anderen auszugeben und es könnte jemand fälschlicherweise behaupten, er wäre der berechtigte Empfänger und Ihnen seinen Public Key andrehen wollen. Er könnte dann die vertrauliche Botschaft lesen. Würde er sie danach, vielleicht auch noch gefälscht, an den richtigen Empfänger weiterleiten, bliebe das ganze wahrscheinlich auch noch unbemerkt.

Diese Problematik lässt sich mithilfe einer **Public Key Infrastructure** (PKI) verhindern.

PKI und Digitale Signatur:

Besonderes Merkmal der **Public Key Infrastructure** (PKI) ist die **Zertifizierungstelle**. Das ist eine allgemein anerkannte Stelle, deren Aufgabe es ist, die jeweils **einmaligen Schlüsselpaare** (privater und öffentlicher Schlüssel) natürlichen Personen fest zuzuordnen und dies den Benutzern mittels **"Zertifikaten"** zu bestätigen.

Vereinfacht funktioniert das ganze so: Jeder Benutzer kennt den Public Key der Zertifizierungsstelle. Aber nur sie hat den passenden Private Key für eine sinnvolle Verschlüsselung als Gegenstück dazu. Jetzt erfolgt das Gegenteil vom bisherigen Verschlüsseln einer Nachricht. Die Zertifizierungsstelle erstellt einen Text, in dem der öffentliche Schlüssel einer Person zugeordnet wird, und verschlüsselt dies aber mit ihrem geheimen Schlüssel. Weil der öffentliche Schlüssel der Zertifizierungsstelle allen bekannt ist, kann diesen Text auch jeder lesen.

Und wozu das ganze? Jeder weiß nun genau, dass die Zertifizierungsstelle diesen Text geschrieben hat - nur sie kann mit ihrem Private Key Nachrichten so verschlüsseln, dass mit dem allen bekannten Public Key wieder eine sinnvolle Nachricht dabei herauskommt. In diesem Fall hat die Zertifizierungsstelle eine Nachricht geschrieben und digital mit ihrem privaten Schlüssel "signiert". Sofern Sie der Zertifizierungsstelle vertrauen, können Sie dann auch darauf vertrauen, dass dieser Public Key einer ganz bestimmten Person gehört.

Die so erfolgte digitale Signatur ist also keine digitalisierte "echte" Unterschrift, sondern ein Bitmuster, das mittels eines mathematischen Verfahrens erstellt wird. Eine digitale Signatur können auch Sie erstellen, wenn Sie ein gültiges Schlüsselpaar aus öffentlichen und privaten Schlüssel besitzen. Sie brauchen aber die Zertifizierungsstelle, die bestätigt, dass Sie und kein anderer zu Ihrem Public Key gehören.

Mithilfe der PKI können Sie nicht nur Nachrichten sicher verschlüsseln, um deren Inhalt vor neugierigen Zeitgenossen zu verbergen. Die digitale Signatur verhindert auch, dass Nachrichten unbemerkt verändert werden.

Sehen Sie sich einfach diesen Text mit der anschließenden Zahl an:
[Angriff im Morgengrauen 21/207]
Die 21 steht für die Anzahl der Buchstaben im Text und die 207 für den Wert der Buchstaben, wenn man diese nach Ihrer Stellung im Alphabet addiert. Aus dem Text lassen sich die Zahlen leicht ermitteln, aber nicht umgekehrt. Mithilfe der PKI kann man den Text und die Zahlen verschlüsseln und mit der Nachricht gleich mitschicken. So wird der Empfänger merken, ob irgend etwas manipuliert wurde. Sonst würden die Zahlen nicht mehr zum Text passen. Allerdings gibt es dabei noch einen Haken: Wer

den Text manipuliert, kann natürlich auch die so Zahlen manipulieren, dass sie wieder zum Text passen. Damit das nicht passiert, werden die Zahlen mit dem geheimen Schlüssel des Absenders verschlüsselt. Das noch genauer zu erklären, würde an dieser Stelle aber nun wirklich zu weit führen.

Kombiniert man schließlich alles, erhält man ein tolles Ergebnis: Niemand kann unbemerkt die Nachrichten fälschen, lesen oder sich für jemanden anderen ausgeben. Das ist doch prima, oder?

Anwendung der Verschlüsselungsverfahren

Viele private Nutzer verwenden das Programm **Pretty Good Privacy** - abgekürzt **PGP** (deutsch: ganz gute Vertraulichkeit) - für die Verschlüsselung ihrer E-Mails und Dateianhänge. PGP beruht einem **hybriden Verschlüsselungsverfahren**: Um Nachrichten zu verschicken, werden diese mit dem entsprechenden öffentlichen Schlüssel des Adressaten verschlüsselt. Der kann die Nachricht dann mit dem geheimen Schlüssel dechiffrieren.

Neben dieser kommerziellen Software gibt es auch noch **Gpg4win** (Gnu Privacy Guard für Windows) ein vom BSI gefördertes Freies Software Projekt. Mit dieser Open-Source-Software kann man ebenfalls E-Mails und Dateien sicher, vertrauenswürdig, einfach und kostenlos verschlüsseln - unabhängig von den jeweiligen Datenformaten (E-Mail, Textdateien, Bilddaten, usw.). GnuPG ist kompatibel zu PGP, das heißt mit GnuPG verschlüsselte E-Mails können mit PGP entschlüsselt werden und umgekehrt. GnuPG verwendet dazu hauptsächlich ein hybrides Verfahren und arbeitet mit Public Keys. Zum Verschlüsseln kann GnuPG aber wahlweise ausschließlich mit symmetrischen Verfahren eingesetzt werden.

Eventuell haben Sie in diesem Zusammenhang auch schon einmal etwas von Gpg4win (Gnu Privacy Guard für Windows) gehört. Gpg4win ist ein Projekt, dass die Verwendung von GnuPG auf dem am meisten verbreiteten Betriebssystem Windows vereinfachen will. Denn GnuPG ist eine so starke Verschlüsselungstechnologie, dass eine breite Öffentlichkeit - also auch alle Windows-Anwender - sie in Zukunft nutzen soll.

Zum Schluss noch zu "echten" Anwendungen der **Digitalen Signatur** (oder juristisch korrekt der "Elektronischen Signatur"): Wie bereits gesagt, soll durch sie der Ersteller eines elektronischen Dokuments erkennbar sein und die Dokumente vor unbemerkten Veränderungen geschützt werden. Die mit der elektronischen Signatur unterschriebenen Rechtsgeschäfte (Verträge, Steuererklärungen, etc.) sollen natürlich auch dauerhaft und beweisbar rechtsgültig sein. Deshalb wurden im Signaturgesetz Qualitätsstufen festgelegt. Die regeln die dafür notwendigen Details. **Die im Signaturgesetz definierte qualifizierte elektronische Signatur ist durch Gesetzesänderungen zukünftig auch formal als Ersatz der eigenhändigen Unterschrift zugelassen**. In zahlreichen Pilotversuchen in Wirtschaft und Verwaltung wird diese neue Technologie derzeit schon erprobt.

Das waren jetzt ziemliche viele Informationen auf einmal. Vielleicht konnten wir Sie aber davon überzeugen, dass das mit der Verschlüsselung eine ganz nützliche Sache ist. Wenn Sie wollen, können Sie es auch gleich selbst ausprobieren: In der Toolbox finden Sie ein Verschlüsselungsprogramm. Dann sehen Sie gleich, wie es in der Praxis funktioniert. **Zur Erinnerung**: Die Sicherheit Ihrer Nachrichten hängt von der Wahl eines originellen - also schwer zu erratenden - und nicht zu kurzen Schlüssels ab.

Patch-Management

Patchen, damit Computer, Handy & Co. sicher bleiben.

Ob Betriebssysteme für PC und Laptop, Mediaplayer für das Abspielen von Audio- und Videodateien, Software für Handys oder auch das Virenschutzprogramm – sie alle bieten nur dann sicheren Schutz vor Computerschädlingen, wenn sie auf aktuellem Stand sind. "Patch", der englische Ausdruck für "Flicken", heißt das Zauberwort: Dahinter verbergen sich kleinere oder größere Softwarepakete, mit denen die Hersteller Sicherheitslücken in ihren Programmen schließen oder andere Verbesserungen integrieren. Unter Sicherheitslücken versteht man dabei Schwachstellen in Software, die es Angreifern beispielsweise ermöglichen, bösartige Programme einzuschleusen und die Kontrolle über fremde Systeme zu übernehmen. Da viele Nutzer heutzutage zahlreiche verschiedene Softwareprodukte einsetzen, wird es immer schwieriger, den Überblick zu bewahren. Bei manchen Programmen, etwa Betriebssystemen wie Mac OS X und Windows, erleichtern automatische Update-Services die Aktualisierungsarbeit. Bei vielen Anwendungen, z. B. dem Virenschutz, ist dies auch schon längst Standard. Vielfach ist es aber der Verantwortung der einzelnen Nutzer überlassen, neue Entwicklungen zu verfolgen und die Software durch das Herunterladen und Installieren von Patches vor Viren, Würmern und sonstigen Angriffen zu sichern – zumindest solange, bis der nächste Computerbösewicht eine vom Hersteller bisher übersehene Lücke findet. Mit unserem Leitfaden wollen wir Sie dabei unterstützen, ohne allzu großen Aufwand ein System in Ihr Patch-Management zu bringen und sich damit vor bösen Überraschungen zu schützen.

Leitfaden für sicheres Patch-Management

Beachten Sie die folgenden Maßnahmen, damit Computer, Handy & Co. immer auf dem aktuellen Stand sind und bleiben.

Verschaffen Sie sich einen Überblick über die wichtigsten von Ihnen eingesetzten Programme!

Dazu zählen neben dem Betriebssystem und dem Browser auch Office-Pakete, Medienplayer, Dienstprogramme von Providern oder das Virenschutzprogramm. Das gilt nicht nur für den PC, sondern auch für die auf dem Laptop, dem PDA oder dem Handy installierten Programme.

Prüfen Sie, ob bzw. zu welchen Produkten Sie automatische Update-Services erhalten!

Wenn Sie nicht ohnehin wissen, von wem Sie regelmäßig automatisch Updates erhalten, dann nehmen Sie sich kurz Zeit und sehen Sie in Ihrem Softwarevertrag oder in der Online-Hilfe beziehungsweise in den Einstellungen Ihrer Software nach. In der Regel hat man mit der Software einen Anspruch auf ein Jahr technische Unterstützung (Support) und Aktualisierungen bzw. Patches erworben.

Machen Sie es sich zur Regel, Hinweise auf Updates zu beachten und nicht wegzuklicken!

Die große Zahl unerwünschter Werbe-Popups, mit denen man als Internetnutzer konfrontiert wird, kann dazu führen, dass man jedes Popup einfach weg klickt. Machen Sie es sich zur Gewohnheit, eine kurze Kontrollsekunde einzulegen und prüfen Sie, ob es sich dabei nicht vielleicht doch um einen wichtigen Warnhinweis handelt.

Erstellen Sie eine Übersicht darüber, für welche Programme Sie eigenständig auf Updates achten müssen!

Falls Sie feststellen, dass Ihnen für eines oder mehrere zentrale Programme kein automatischer Update-Service zur Verfügung steht, lohnt sich das Anlegen einer Liste. So wissen Sie, welche Produktinfos für Sie von Bedeutung sind.

Informieren Sie sich regelmäßig über Updates – etwa durch Newsletter oder Branchenplattformen!

Das Bürger-CERT des BSI bietet ein Newsletter-Service an, der Sie über wesentliche Neuerungen informiert [www.buerger-cert.de]. Aber auch einzelne Softwareproduzenten oder Brancheninformationsdienste wie www.heise.de oder www.golem.de stellen Warndienste ("Alert Services") per E-Mail und Newsticker zur Verfügung.

Laden Sie Patches rasch herunter und installieren Sie sie!

Computerbösewichte wissen, dass zumeist schon bald nachdem eine Sicherheitslücke bekannt wird Patches zur Verfügung stehen. Daher versuchen Sie, die Schwachstellen gleich in den ersten Tagen auszunutzen, indem sie Schädlinge wie Viren und Würmer programmieren und in den Umlauf bringen. Nur so können sie soviel Schaden wie möglich verursachen – oder auch maximalen Profit machen. Daher sollten Sie darauf achten, Patches so rasch wie möglich herunter zu laden und zu installieren!

ACHTUNG: Lassen Sie sich durch gefälschte Updates nicht aufs Glatteis führen!

Leider wird die Bereitschaft zum Patch-Management durch die Programmierer von Computerschädlingen immer wieder für Ihre Zwecke missbraucht: So werden etwa Warn-E-Mails gefälscht und irreführende Popups auf fremde Computer geschmuggelt. Als Richtschnur sollten Sie Updates nur dann installieren, wenn der Hinweis darauf in der Ihnen vertrauten Form erfolgte. Wenn Ihnen E-Mail-Nachrichten mit Aktualisierungshinweisen verdächtig erscheinen, dann folgen Sie den darin enthaltenen Links nicht, sondern informieren Sie sich in Newstickern und tippen Sie die entsprechenden Webadressen manuell ein. Grundsätzlich sollten Sie keine Mailanhänge mit angeblichen Aktualisierungen bzw. Patches öffnen, denn seriöse Firmen verschicken solche Daten nicht per E-Mail.

Achten Sie auf Mitteilungen, die das Auslaufen des Supports für Produkte ankündigen!

Softwareanbieter bieten Aktualisierungen für einzelne Produkte oftmals nur für einen gewissen Zeitraum an. Beispiel dafür ist etwa die Beendigung des Supports für Windows 98 und für Windows XP (mit Service Pack 1) durch Microsoft. Auch darüber können Sie sich durch regelmäßigen Besuch der Anbieter-Webseiten oder in Branchendiensten informieren.

Installieren Sie, wenn erforderlich, Upgrades für neue Programmversionen!

Wenn Hersteller umfassende Änderungen an Ihren Programmen vornehmen, dann erhalten diese Aktualisierungspakete oft eine neue Versionsbezeichnung. Das Programm x in der Version 1.2 wird also beispielsweise durch die Installation eines Upgrades zur Version 1.3. Zumeist sind in solchen Upgrades auch sicherheitsrelevante Änderungen enthalten.

Beispiel "Microsoft Update"

Anhand von "Microsoft Update" lässt sich beispielhaft darstellen, wie Patch-Management für Privatpersonen funktioniert. Nähere Informationen dazu finden Sie auch auf den Webseiten von Microsoft. Hier haben wir für Sie die wichtigsten Punkte zusammen gefasst.

Was ist Microsoft Update?

Microsoft bezeichnet damit einen Teil seiner Webseite, auf dem die neuesten Updates für all seine Programme – vom Betriebssystem Windowsüber den Browser Internet Explorer bis hin zu Outlook oder dem Movie Maker – bereit gestellt werden.

Wie stellen Sie fest, ob Sie Aktualisierungsbedarf haben?

Ihren Update-Service finden Sie je nach Betriebssystemversion unter Start > (Einstellungen) > Systemsteuerung. Bei manchen Betriebssystemen sehen Sie an dieser Stelle schon den Hinweis "siehe auch Windows Update" mit einem entsprechenden Link. Wenn kein Hinweis auftaucht, so gehen Sie weiter zu → Software → neue Programme installieren → Windows Update". Ihr Computer wird danach automatisch auf veraltete Software überprüft, die entsprechenden Updates werden Ihnen zum Download angeboten. Nach Updates für Microsoft-Office-Programme wie Word, Excel oder PowerPoint können Sie übrigens unter der Funktion Office Update suchen.

Wie installieren Sie die Updates?

Markieren Sie die Kästchen neben den Updates, die in der Liste angeführt werden und klicken Sie auf "Updates installieren".

Wie automatisieren Sie den Update Service?

Wenn Sie Windows XP mit dem Service Pack 2 nutzen, ist die Funktion "Automatische Updates" möglicherweise bereits aktiviert. Für alle anderen Windows-Versionen – mit Ausnahme von Windows 95, Windows 98 und Windows NT – kann die automatische Funktion über die Webseite von Microsoft Update aktiviert werden.

Was müssen Sie selbst noch tun, wenn Sie automatische Updates beziehen?

Sie können selbst einstellen, in welchem Umfang Sie am Update-Vorgang beteiligt sein wollen. Je nachdem startet Ihr PC nach dem Download neuer Updates sofort mit dem Installationsvorgang oder informiert Sie mit einer Info bzw. einem Warnhinweis. In diesem Fall können Sie dann selbst aussuchen und anklicken, was installiert werden soll.

Was ist der Microsoft Patch-Day?

An jedem zweiten Dienstag im Monat (durch die Zeitverschiebung zwischen den USA und Europa bei uns meist spät abends) veröffentlicht Microsoft jüngste Aktualisierungen. Wenn dringender Handlungsbedarf besteht, wird dieser Rhythmus allerdings auch durchbrochen.

Service Pack 2 für Windows XP

Je komplizierter eine Software ist, desto größer die Gefahr, dass sich darin Programmierfehler – Bugs – einschleichen. Die Hersteller versuchen die Bugs ständig zu korrigieren, indem sie so genannte Patches anbieten. Um die Installation von sehr vielen, einzelnen Patches zu vermeiden, werden im Abstand von einigen Monaten alle bis zu diesem Zeitpunkt verfügbaren Patches zu einer Patch-Sammlung, einem so genannten Service Pack, zusammengefasst. Mit dem "Service Pack 2" können Sie Ihr Betriebssystem Windows XP aktualisieren. Und das sollten Sie auch tun! Denn mit dem Betriebssystem-Update von Microsoft werden zusätzlich zu den Patches eine ganze Reihe neuer Sicherheitsfunktionen installiert und eingerichtet.

Doch bevor Sie loslegen: Führen Sie vor der Installation des Service Pack 2 unbedingt eine Datensicherung durch. Wenn - wider Erwarten - irgend etwas schief gehen sollte, können Sie so den ursprünglichen Systemzustand wiederherstellen.

Die wichtigsten Neuerungen, die das Service Pack 2 mitbringt, im Überblick:

- Zentrales Sicherheitsmanagement
- Größerer Netzwerkschutz
- Optimiertes Speichermanagement
- Höhere Sicherheit bei der E-Mail und Internetkommunikation

Zentrales Sicherheitsmanagement

Alles im Blick. Im neuen **Sicherheitscenter** können folgende Funktionalitäten zentral überwacht werden:

- Automatische Updates
- Viren-Scanner
- Windows-Firewall

Größerer Netzwerkschutz

Die **Windows-Firewall** ist nach der Installation der Service Pack 2 für Windows XP standardmäßig aktiviert. Die Firewall muss erst einmal an die eigenen Bedürfnisse angepasst werden. Das heißt, man muss genau festlegen, wer an wen und auf welchem Weg welche Daten versenden darf. Klappt einmal gar nichts mehr oder hat man den Überblick verloren, kann man die Firewall-Einstellungen auf einen Standardwert zurücksetzen.

Optimiertes Speichermanagement

Eine so genannte **Datenausführungsverhinderung** hilft vor bestimmten Angriffen zu schützen. Der Name erklärt sich fast von selbst. Durch diese Funktion wird verhindert, dass ein Angreifer “bösartigen” Code ausführen darf, welchen er durch eine Attacke in den Speicher des Opfer-Rechners lädt. Sie kennzeichnet gewisse Speicherbereiche als “nicht ausführbar”.

Höhere Sicherheit bei der E-Mail- und Internetkommunikation

Bei der Nutzung von **Outlook** beziehungsweise **Outlook Express** können E-Mails anstelle der Anzeige in HTML auch als unformatierter Text dargestellt werden.

Die Anzeige von in E-Mails eingebetteten **Bildern**, die einen Kontakt zu Webservern herstellen könnten, kann **blockiert werden**. Dies verhindert die Verifikation von E-Mail-Adressen durch Spammer. Das heißt der Spammer weiß nicht, ob Sie die E-Mail empfangen haben.

Ebenso warnt ein **Dateiausführungsschutz** vor der Ausführung von Dateien aus nicht vertrauenswürdigen Quellen, sofern diese mit Microsoft Programmen wie beispielsweise dem Internet Explorer heruntergeladen wurden.

Die **Internet Explorer Informationsleiste** bietet eine zentrale Stelle, um zum Beispiel Aktive Inhalte, Pop-Up-Fenster, etc. zu blocken.

Wie das ganze genau funktioniert, eine detaillierte Installationsanleitung und viele weitere Informationen erhalten Sie direkt auf den Internetseiten von Microsoft.