Vorwort

Folgende Texte stammen von www.dischue.de und beschäftigen sich mit den Themen Internet und PC sowie damit zusammenhängend Sicherheit und Datenschutz. Die Texte wurden ohne große Veränderungen von der Webseite übernommen. Durch die Umwandlung in ein OpenOffice-Dokument und anschließendes Ausdrucken als pdf ist es möglich, dass einige Links Probleme machen – vor allem trifft das auf das Bild mit Browserversion, Betriebssystem und IP zu -dieses funktioniert nur auf der o.g. Webseite korrekt.

Die etwas ungünstige Formatierung ist dem kopieren und einfügen ohne große Nachbearbeitung geschuldet.

PC und Internet Teil 1: Datensicherheit

Veröffentlicht am 30/01/2012 von dischue

Da ich gelegentlich mal gefragt werde, was man am PC und im Internet so beachten soll, habe ich mich mal ran gesetzt und folgenden kleinen Beitrag getippt. Ich bin da auch nicht der große Auskenner – Freunde und Bekannte fragen trotzdem. Um es vorneweg zu sagen: Anleitungen zu diesem Thema gibt es wie Sand am Meer – dies ist nur eine mehr…. Es schadet natürlich nicht, sich bei mehreren Quellen kundig zu machen. Ich habe hier versucht, Grundsätzliches ohne Fach-chinesisch zu erklären – ich hoffe, es klappt. Wer wirklich genug Ahnung hat, kann sich diesen Artikel hier sparen – oder mich verbessern, sollte ich zu sehr daneben liegen. Beim Schreiben habe ich allerdings gemerkt, dass ich hier vom Hundertsten zum Tausendsten komme, deshalb habe ich das Ganze in mehrere Teile aufgefächert. In den ersten Teilen versuch ich, bestimmte Bereiche abzuarbeiten, in den letzten Teilen werden dann zunehmend Zusammenhänge sichtbar – hoffe ich.

Auch wenn es öde ist, mal kurz Theorie zur Unterscheidung ein kluger Satz aus der Schule: unterschieden wird zwischen Datensicherheit und Datenschutz. Datensicherheit ist eigentlich recht simpel: die Daten sollen eben sicher sein – sicher vor Verlust und/oder Beschädigung. Wie bei einem normalen Fotoalbum: es soll nicht beschädigt werden, es soll nicht verloren gehen. Obwohl bei Computern bzw. digitalen Daten leicht für Datensicherheit gesorgt werden kann, denken viel erst daran, wenn es zu spät ist. Dabei wäre schon viel damit getan, alle paar Tage/alle 2 Wochen/einmal im Monat wichtige oder lieb gewonnene Daten z.B. auf eine externe Festplatte zu kopieren. (CD oder DVDs brennen dauert zu lange und selten passt alles auf eine Scheibe) Geht der Computer kaputt, sind die Daten auf der externen Festplatte noch vorhanden – selbst wenn die Daten der letzten 14 Tage fehlen sollten, ist das immer noch besser, als wenn alle Daten verloren wären. Manch einer wird jetzt noch ausführen: die externe Festplatte sollte woanders aufbewahrt werden, als der Computer, damit bei Brand oder Einbruch nicht beides beschädigt oder gestohlen wird. Völlig korrekt – aber vielen wäre schon allein mit einer externe Festplatte geholfen.

Abbildung 1: 2 kleine (2,5 Zoll) externe Festplatten. Vorteile: benötigen kein Netzteil da Versorgung über USB, recht handlich, Nachteile: wie alle Festplatten: Vorsicht bei Betrieb vor Erschütterungen

Was also machen? *Am einfachsten in regelmäßigen Abständen seine Daten auf eine externe Festplatte kopieren.*

Welche Daten sollen kopiert werden? - *Die Daten, die einem lieb und teuer sind: Fotos, Musik, Videos, persönliche Dokumente wie wichtige Schreiben (Lebenslauf, Bewerbung, Kopien von Verträgen, Rechnungen, Steuererklärung…)*

Wie sicher ich? – *Die Ordner, die die Daten enthalten, am einfachsten auf die externe Festplatte kopieren.*

Wo finde ich die Ordner? *Wenn an dem Computer nicht selbst etwas geändert wurde, so liegen die Ordner wahrscheinlich unter C:\Dokumente und Einstellungen\Computer bzw. Kontoname\Eigene Dateien… (hier also der Name des Computers oder des Kontos, mit dem man angemeldet ist). Standardmäßig werden Dateien in den entsprechenden Ordnern gespeichert: Bilder in "Eigene Bilder", Videos in "Eigene Videos", Briefe/Tabellen in "Eigene Dokumente" usw… Diese Ordner (oder den gesamten Ordner "Eigenen Dateien" – dabei sind aber Fehlermeldungen möglich) einfach kopieren. Außerdem noch den Ordner "öffentliche Dateien" mit den entsprechenden Unterordnern "Musik", "Bilder" usw… Außerdem natürlich alle Ordner sichern, in welchen man außerdem noch wichtige Dateien abgespeichert hat.*

Abbildung 2: USB-Sticks, Vorteile: klein und handlich, keine bewegten Teile; Nachteile: Preis je Speichergröße höher als bei Festplatten, leicht zu verlieren, oft recht langsame Datenübertragung. Ausreichend, um z.B. die letzten Urlaubsbilder mit zu Freunden zu nehmen.

Wenn gefragt wird, ob bestehende Daten überschrieben werden sollen: in diese Richtung (Computer –> externe Festplatte) sollen sie – also "ja". Dafür genügt der Windows Explorer, meiner Meinung nach komfortabler geht es mit Dateimanagern wie FreeCommander oder Total Commander. Es gibt auch unzählige Programme, die das automatisieren können, also ältere oder auf dem Computer gelöschte Daten auf der externen Festplatte automatisch löschen, Dateien vergleichen usw. Genannt seien hier mal Backup Slave und Dirsync, beide für Privatanwender kostenlos. Oft liegen externen Festplatten oder Speichersticks auch solche Programme bei. Bitte aber erst mit einem Testordner probieren, um sich in das jeweilige Programm einzuarbeiten!

Wichtig: keine Ordner kopieren, die eine kleinen Pfeil im Symbol haben – das sind nur Verknüpfungen, die "zeigen" lediglich auf den richtigen Ordner (meist auf den Desktop vorhanden). Sollte also nach 2 Sekunden alles kopiert sein – dann stimmt was nicht. Wäre nicht das erste Mal, dass Verknüpfungen gebrannt oder kopiert werden… Also wenigstens den Explorer benutzen

und schön schauen, wo welche Ordner liegen…

Man kann das Ganze ja wie erwähnt automatisieren – es gibt genügend (auch kostenlose) Programme (z.B. die oben genannten), die eine automatische Sicherung (“Backup”) ermöglichen – zeitgesteuert oder z.B. immer beim Verbinden mit der externen Festplatte. Für persönliche Dokumente, wichtige Kopien usw. bietet es sich u.U. auch an, diese Daten (verschlüsselt!!) zusätzlich “in der Cloud” (im Internet) abzulegen. Ich denke da z.B. an Kopien von Dokumenten oder Urkunden, Bewerbungsschreiben, Abschlüssen o.ä. – allerdings sind solche Kopien rechtlich oft nicht gültig. Ich halte aber eine Kopie immer noch für besser, als keine Kopie (nur persönliche Meinung, zum Glück noch nicht verwenden müssen). Anbieten würden sich diverse, kostenlosen Speicher, Microsofts Skydrive, die Telekom Cloud (für Telekom-Kunden kostenlos) Dropbox, Stratos HiDrive (kostenlos bis 30 GB) u.a. Die Bedienung und Leistungsmerkmale unterscheiden sich natürlich von Anbieter zu Anbieter.

Abbildung 3: Festplatten-Dockingstationen: nehmen je Modell 1 oder mehrere interne Festplatten verschiedener Größe auf. Vorteile: Verschiedene Anschlüsse auch kombiniert möglich (USB 2.0, USB 3.0, eSATA) Festplatten lassen sich leicht tauschen, nur 1 Netzteil (der Dockingstaion) für alle Festplatten (statt bei externen 3,5 Zoll Platten oft verschiedene Netzteile). Je nach Modell auch 1:1 Kopie von Festplatten ohne PC möglich (rechtes Modell). Nachteile: wie bei allen Festplatten: Vorsicht mit Erschütterungen bei laufender Platte.

Manch ein “Profi wird jetzt müde lächeln – falls er bis hier gekommen ist. Da werden jetzt Stichworte fallen wie “Raid-System” aufbauen, Home-Server einrichten oder ein NAS – aber wie eingangs erwähnt, sollte es um einfache Möglichkeiten gehen. Und während ein ständig laufendes NAS und /oder Home-Server bei einer Überspannung (Blitzeinschlag) genau so geschädigt werden können, wie der Computer selbst, liegt die externe Festplatte im Schrank und bekommt vom

Gewitter nichts mit. Die einfachsten Mittel müssen nicht die schlechtesten sein. Für viele, die mal eine defekte Festplatte hatten, wäre es schon gut genug gewesen, sie hätten wenigstens überhaupt eine Sicherung gehabt – aber da kommt man oft erst drauf, wenn es zu spät ist.

Übrigens: (versehentlich) gelöschte Dateien lassen sich natürlich aus dem Papierkorb wieder herstellen. Aber auch, wenn der Papierkorb geleert wurde, sind die Dateien noch auf der Festplatte – sie haben lediglich die Kennzeichnung, dass sie überschrieben werden können – noch sind sie also zu retten. Am allerbesten von einem anderen PC aus oder in dem der betroffenen Computer mittels eines "Notsystems" (Linux, Win PE, Knoppix) von USB-Stick oder CD gebootet wird. Das verhindert, dass die Dateien gerade beim Rettungsversuch überschrieben werden. Zu Rettung benutzt man dann Tools wie Recuva oder Photorec u.ä. – klappt es mit dem einen Tool nicht, versucht man es mit dem nächsten. Das funktioniert auch mit versehentlich gelöschten oder formatierten Speicherkarten aus Digitalkameras u.ä.

Im nächsten Teil geht es dann ein wenig um Ungeziefer auf dem PC – also Viren, Würmer und Trojaner und was man da (vorher) tun kann. außerdem wird das Thema Router leicht angeschnitten – falls ich nicht nochmal alle Entwürfe über den Haufen werfe… 

PC und Internet Teil 2: Virenschutz und Router

Veröffentlicht am 06/02/2012 von dischue

Im ersten Teil ging es ja um Datensicherheit. Hier soll es nun um ein paar kleine, grundlegende Dinge gehen, den eigenen PC sicherer zu machen. Es gibt ja auch Viren, Würmer und Trojaner – vereinfacht einfach Schadprogramme. Was die machen? Unterschiedlich – "früher" haben die den Computer verlangsamt, einfach Daten gelöscht und anderen Unsinn. Heute arbeiten die vor allem unerkannt im Hintergrund, wollen Passwörter abfragen oder über den befallenen PC Spam-Mails verteilen, DoS-Atacken auf bestimmte Wegseiten ermöglichen (durch tausende, gleichzeitige Aufrufe einer Webseite diese überlasten) oder andere unschöne oder illegale Dinge tun.

Wie im echten Leben gibt es keine 100%ige Sicherheit. Ein Computer wäre nur dann (annähernd) 100%ig sicher, wenn ich damit nicht ins Internet gehe, keine CD/DVD einlege, keinen USB-Stick anschließen, keine Kamera und keine Speicherkarte – nur was will ich dann damit noch?

Im "realen" Leben kann nur "absolut" sicher vor Einbrechern sein, wenn niemand meine Adresse kennt, keiner das Haus sieht, ich nicht Wohnung/Haus/Garten verlasse – wie soll das gehen?Ich will aber niemanden entmutigen, man kann sich natürlich schützen bzw. es den Bösen so schwer wie möglich machen – im realen Leben (Zaun, Türschloss, Alarmanlage) wie auch am PC und im Internet. Bei Letzteren sind die Schlagwörter dann Firewall und Antiviren-Programm.

Kurz zu Antivirenprogrammen: es gibt kostenlose, die ebenso gut sind, wie kostenpflichtige. Allerdings ploppt dann je nach Anbieter öfter ein Werbefenster auf, man solle doch bitte auf die Bezahlversion umsteigen. Außerdem kann oft nur einmal am Tag upgedated werden - das wären oft schon die Unterschiede. Von der Arbeitsweise, der Engine (sozuagen der inneren Maschine) sind die kostenlosen und kostenpflichtigen Versionen eines Herstellers oft identisch. Den Mehrwert, den komplette Suiten (mit Zusatzfunktionen wie Firewall, Mail-Check u.ä.) bieten, kann man oft vernachlässigen: zumindest lt. ct sind die Firewalls dieser Suiten oft schlecht eingestellt, die Mail-Guards funktionieren oft nicht mit Email-Konten, bei denen die Übertragung verschlüsselt abläuft (TSL/SSL). Also keine Sorge: ein kostenloses Antivir ist nicht unbedingt schlechter als ein zu bezahlendes.

Welches Programm man wählt, ist Geschmackssache – ob die kostenlosen Microsoft Essentials, Avira Antivir, Avast, AVG Anti Virus free, Panda Antivirus, ….. egal. Aber Vorsicht! wer sich nicht auskennt, sollte mal im Bekanntenkreis fragen und nicht das erstbeste kostenlose Programm aus dem Internet installieren – gelegentlich sind genau die Programme, die Schutz versprechen, selbst das Problem – wie ein falscher Polizist.

Kein Programm kennt alle Viren, die im Umlauf sind und manchmal wird auch eine "saubere" Datei fälschlich als Virus erkannt ("False positiv"), man sollte also Funde nicht sofort löschen lassen sondern erst mal in Quarantäne schicken. Den Speicherort auf jeden Fall merken! Solche Dateien kann man dann z.B. zu jotti hochladen. Dort werden sie mit mehreren Antiviren-Programmen getestet. Es wird dann angezeigt, wie viel der Programme die Datei als Virus erkennen und wie viel nicht. Dann muß man allerdings abwägen: erkennen nur wenige Programme ein Virus, ist es wahrscheinlich ein Fehlalarm – oder ein brandneuer, noch unbekannter Virus…. Was man trotzdem auf keinen Fall machen sollte: mehr als 1 Antiviren-Programm installieren. das bringt nicht mehr Sicherheit sondern macht nur Ärger – da sich die Programme gegenseitig behindern würden. Im schlimmsten Fall hält ein Programm das jeweils andere für einen Virus und legt den PC lahm.

Dummer Weise installieren oder "öffnen" viele noch selbst Schadprogramme – ein uralter Trick der bösen Jungs ist immer noch wirksam: ein solches Programm wird per Email versendet. Im Betreff

steht oft “Rechnung” oder “wichtig” oder “Mahnung”. Im Text dann kurz “Vielen Dank für ihre Bestellung…” oder “sie vergaßen sicherlich…” mehr Details kann man dann angeblich im Anhang erfahren. Und schon klickt der eine oder andere auf den Anhang und öffnet damit einen Virus oder Trojaner… Viele achten nicht darauf, dass die Datei, auf die sie da klicken z.B. rechnung.exe heißt. Warum sollte eine Rechnung in einer ausführbaren Datei (.exe) stecken? Wenn Rechnungen per Mail kommen, dann in der Regel als pdf! Große Versender legen eher eine “altmodische” Papier-Rechnung der Warensendung bei.

Auch von USB-Sticks oder CDs werden noch Viren versehentlich installiert: seit einigen Windowsversionen blendet Windows standardmäßig die Dateiendung bekannter Dateitypen aus. Und Windows setzt eine Menge als bekannt voraus: bei .exe, .jpg, .mp3 u.ä. wird die Endung nicht angezeigt. Die Datei *bild.jpg* wird also als *bild* angezeigt, eine *setup.exe* als *setup*. Dabei wird als Dateiendung der Teil hinter dem letzten Punkt betrachtet. Bei einer Datei *bild.jpg.exe* wird also immer noch *bild.jpg* angezeigt. Das ist also scheinbar eine harmlose Bild-Datei (das Symbol läßt sich manipulieren) – aber in Wirklichkeit eine u.U. gefährliche exe-Datei. Natürlich ist nicht jede exe gefährlich – aber wenn der Name derartig manipuliert wird, sollte man stutzig werden.

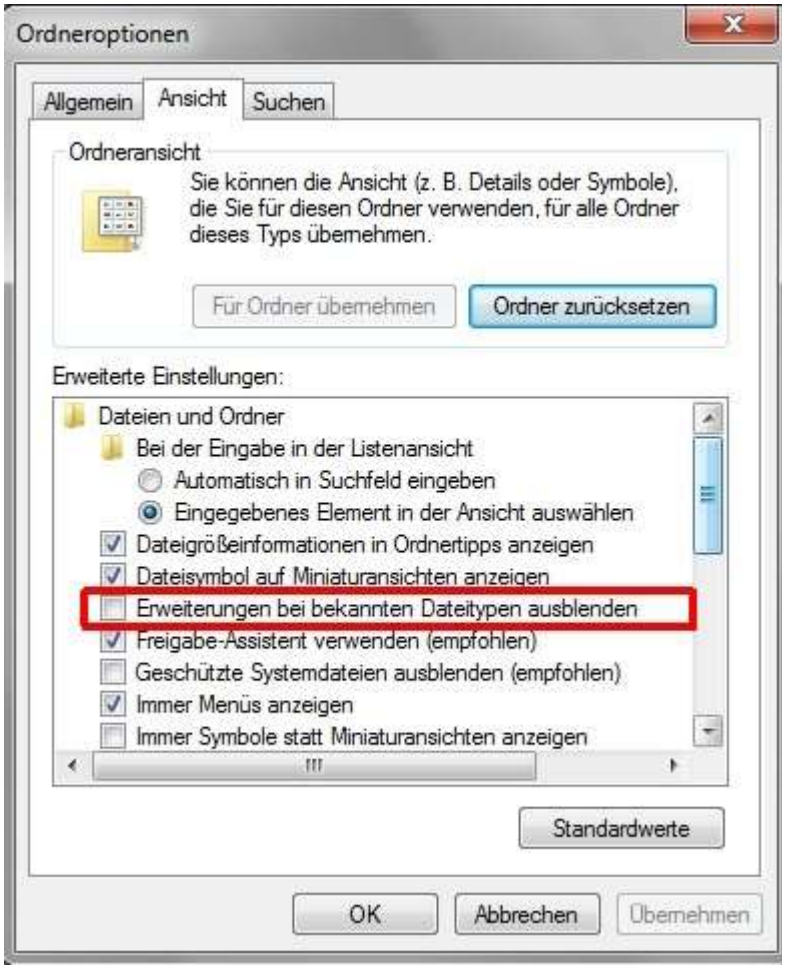


Abbildung 4: Option zum Aus- bzw. Einblenden bekannter Dateierweiterungen unter Windows 7

Was also tun? Bei der eigenen Windowsversion herausbekommen, wo die Funktion “Dateiendung bei bekannten Dateitypen ausblenden” (o.ä.) zu finden ist und den Haken entfernen. Je nach Windows-Version findet man diese Option im Explorer bei Ordner-Optionen. Unter Win 7 in der Suche “Dateierweiterungen” eingeben, der Punkt *Dateierweiterungen ein- oder ausblenden* führt dann zu dem nebenstehendem Bild.

Was ist nun eine Firewall? – im Grunde genommen eine Vorrichtung, die die ein- und ausgehenden Daten kontrolliert. Das kann ein Programm sein (Software-Firewall) oder "Technik" (Hardware-Firewall). Viele brauchen sich darum gar keine Gedanken machen: in vielen Routern ist eine Firewall integriert. Wer also ein Speedport, eine Fritzbox, eine AliceBox o.ä. im Haus hat, hat damit – soweit ich weiß – auch eine mehr oder weniger gute Firewall. Ansonsten hilft ein Blick in die Bedienungsanleitung.

Jedes Gerät, das ins Internet geht, bekommt eine IP bekommt, eine für diesen Zeitraum einmalige Nummer – genaueres dazu in einem späteren Teil dieser kleinen Reihe… So ein Router ist so ein Gerät (im Grunde fast ein Mini-Computer), das auch eine IP bekommt. Der "richtige" Computer ist aber dahinter. "Vom Internet" aus gesehen, ist also erstmal nur der Router mit seiner IP zu sehen – nicht der Computer dahinter! Geht man also auf www.wieistmeineip.de, so wird dort nur die IP des Routers angezeigt.

Der Router wiederum gibt dem an ihm hängendem Computer (oder mehreren) eine jeweils eigene IP. Da das hinter dem Router ist, kann das eine IP sein, die im Internet schon vergeben ist. Allerdings ist für die Geräte hinter einem Router, sozusagen in der Wohnung, ein bestimmter Bereich reserviert – man spricht dann vom privaten Adressbereich. So können die Computer von Nachbarn vom jeweiligen Router durchaus die gleiche Nummer erhalten – nach außen ist jeder Nachbar mit der vom Internetprovider (dem Router) zugeteilten IP identifizierbar.

Also sorgt der Router praktisch dafür, dass der eigentliche Computer im Internet (mit einfachen Mitteln) nicht zu erkennen ist. Geht man nun mit dem Computer auf eine Webseite, so sieht diese die IP des Routers. Allerdings werden andere Daten vom Computer einfach durch geleitet (Betriebssystem, Browser, Sprache).

Kommen dann Daten von der Webseite Richtung Router, so überprüft dieser, ob diese Daten auch wirklich vom Computer angefordert wurden. Wenn ja, werden sie vom Router an den Computer weiter gereicht. Wurden diese Daten nicht vom Computer angefordert, verwirft der Router diese Daten. Versucht also jemand, Daten für einen Angriff auf den Rechner zu senden, so findet er eigentlich nur ein/den Router vor und diese Daten werden vom Router blockiert.

Ein Router funktioniert ähnlich wie ein Postfach – vom Internet ist (fast) nur das Postfach zu sehen, ein Ganove weiß nicht, zu wem es gehört. Er könnte zwar Daten hinterlegen, wenn das Postfach (Router) feststellt, dass diese Daten nicht angefordert wurden bzw. nicht an ein Gerät dahinter adressiert wurden, werden sie gelöscht. Natürlich gibt es aber auch raffiniertere Methoden für einen Angriff – alles nur eine Frage von Aufwand und Nutzen. Den eigenen Router kann man übrigens hier bei heise.de testen. Im Kasten auf der Seite (unter Router/Firewall) auf "Test starten" klicken.

Eine Software-Firewall macht im Prinzip ähnliches – nur eben direkt auf dem PC. Heutzutage ist eine zusätzliche Softwarefirewall aber überflüssig: zum einen, weil der Router diese Funktion übernimmt, zum anderen ist seit Vista eine funktionierende Firewall in Windows integriert. Zumindest lt. ct funktioniert diese besser, als manch eine zusätzliche Firewall (z.B. Zonealarm oder die eines Antivirenprogramms).

Im Teil 3 dieser kleinen Reihe kommen wir dann mal langsam ins Internet – in dem man nicht so anonym ist, wie manch einer glaubt.

PC und Internet Teil 3: keine Anonymität im Internet

Veröffentlicht am 13/02/2012 von dischue

Nach dem vorigen Beitrag zum Thema Viren und Router kommen wir jetzt mal zum eigentlichen Internet. Um es vorneweg zu sagen: was ich hier berichten werde ist technisch weder korrekt noch vollständig – soll aber den Sachverhalt verdeutlichen. Wer völlig falsche Auslegungen meinerseits findet – einfach melden.
Also erst mal: Antiviren-Programm und andere Programme auf dem Computer sollten halbwegs aktuell sein. Es werden immer wieder Sicherheitslücken gefunden und mit Updates behoben – wenn man denn ein Update macht.

Man muß bedenken: man ist im Internet nicht wirklich anonym. Zum einen hat jedes netzwerkfähige Gerät (Netzwerkkarte, Router, WLAN-Stick, Smartphone…) eine eindeutige, nur einmal vergebene MAC-Adresse. Zum anderen fordert man auch ständig Daten (Webseiten, Bilder, Musik…) an – um die Daten geliefert zu bekommen, müssen diese wissen, wo sie hin sollen. Also erhält man von seinem Internetanbieter eine Adresse, die sogenannte IP. Das ist eine 12 stellige Nummer (mit Umstieg auf IPv6 dann 18 stellig), die zeitgleich z.B. nur an 1 Gerät vergeben wird und meistens 24 Stunden gültig ist. Diese Nummer ist in 4 Segmente eingeteilt, jedes davon hat eine bestimmte Bedeutung bzw. repräsentiert einen bestimmten Bereich. Den einzelnen Internet-Anbietern sind bestimmte Bereiche (die tausende oder mehr Nummern ergeben) zugeordnet. Man kann also anhand der IP-Nummer (IP-Adresse) erkennen, über welchen Internet-Anbieter man ins Netz geht. Das geht z.B. über www.wieistmeineip.de. Also anhand der IP kann man den Internet-Anbieter (Telekom, Alice, Kabel D…) und natürlich auch das Land, aus dem man kommt, erkennen. So weiß Youtube, das da jemand aus Deutschland ein bestimmtes Video ansehen will – dies aber “Dank” Gema und/oder anderer Rechteverwerter für deutsche Internetnutzer gesperrt ist. Um es vorweg zu sagen: es gibt gegen alles ein Gegenmittel… Unter Windows sehen wichtige Adressen und Einstellungen z.B. so aus:

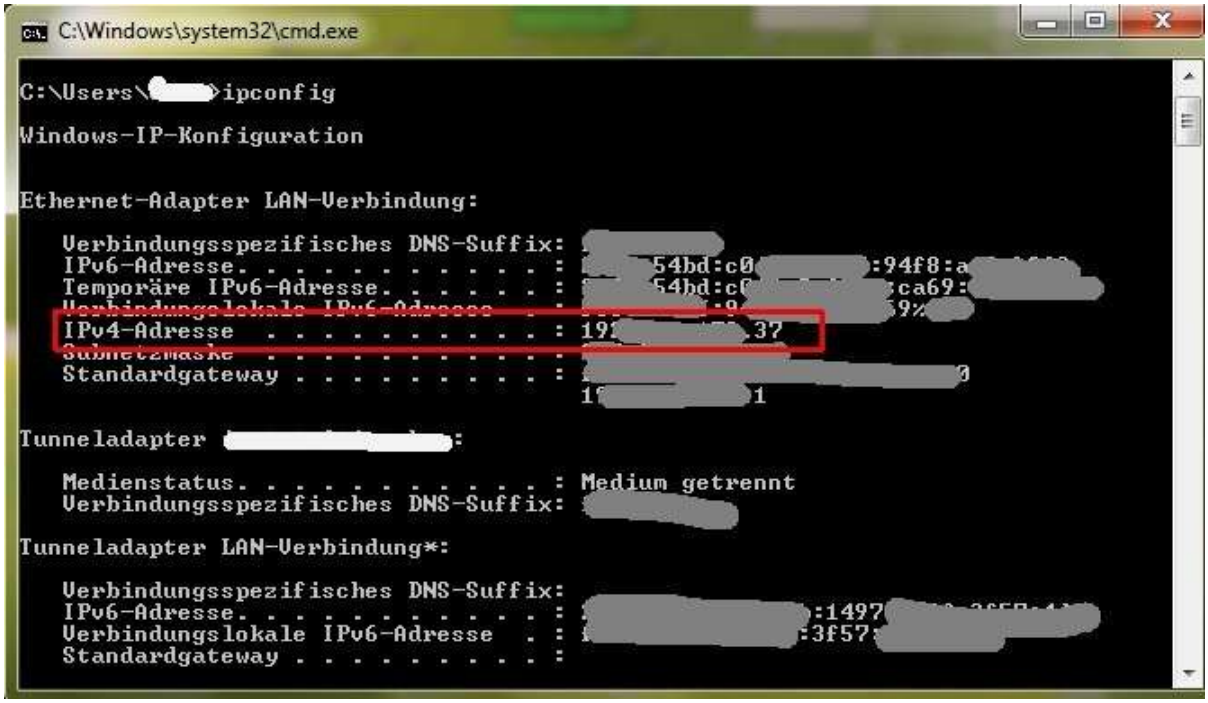


Abbildung 5: Klickt man in Windows auf Start und gibt in die Suchleiste 8oder unter "Ausführen") cmd ein, öffnet sich ein schwarzes Fenster, man kann sofort ipconfig eingeben und erhält in etwa dieses Bild mit Angaben zum Netzwerk/zur IP. Achtung! hier sieht man u.U. nur die IP, die der PC vom Router zugeteilt bekam! Die IP, mit der der Router im Internet "zu sehen" ist, sieht man hier nicht!

Ähnliche Infos gibt es auch in “Bunt”:

Abbildung 6: Man beachte den Pfad: unter Systemsteuerung - Alles Systemsteuerungselemente - Netzwerkübersicht erhält man etwa so eine Abbildung. Zeigt man auf eins der Symbole, werden zusätzliche Infos eingeblendet - hier die IP und die MAC-Adresse. Von links: PC - Router - Internetanbieter. PC und Router haben natürlich jeweils eine andere MAC-Adresse und eine andere IP. Der Router bekommt vom Internetprovider eine eindeutige IP (sozusagen die im Internet sichtbare Anschlussnummer) und vergibt intern selbst an den PC wiederum eine IP. Zeigt man hier auf den PC: IP des PC im eigenen Netzwerk (LAN - Lokales Netzwerk) wird angezeigt. Auf Gateway (mittleres Symbol zeigen): die interne IP des Router wird angezeigt - nicht die, mit der der Router im Internet sichtbar ist!

Aber nicht nur Geräte bekommen eine IP: praktisch jede größere Internet-Seite kann auch über eine IP aufgerufen werden. Mit http://157.150.34.32 kommt man zum Beispiel zur UN (UNO, Vereinte Nationen). Nun lassen sich Zahlen aber oft nicht so einfach merken – deshalb gibt es dann die Adresse www.un.org. Wird diese am PC eingegeben, so fragt der PC über Internet-Anbieter sogenannte Namensserver. Auf diesen speziellen Großrechnern ist hinterlegt, welche IP (also Nummer) zu welcher alphabetischen Internetadresse gehört – oder andersherum. Allerdings gab es gerade einen Virus, der diese Abfrage manipulierte: man wurde nicht zu einem "echten" dieser "Übersetzungsserver" (DNS-Server) geleitet, sondern zu einem manipulierten. In diesem Beitrag steht mehr dazu und hier kann man prüfen (nur noch kurze Zeit), ob der eigene Rechner betroffen ist.

Das wäre also die Sache mit der IP. übrigens wird auch auf meiner kleinen Seite – wie bei sehr vielen anderen auch – die IP-Adresse der Besucher ausgewertet. Dabei werden allerdings bestimmte Stellen der IP nicht verwendet. Eine Zuordnung zu einer bestimmten Person wird nicht vorgenommen. Die Auswertung erfolgt über einen kostenlosen Service von Google. Der sagt mir, wie viel verschiedene Leute (oder besser: Geräte) meine Seite besuchen. Außerdem wird ausgewertet, aus welchem Land die Besucher kommen bzw. sogar aus welcher Gegend bzw. Stadt – allerdings recht ungenau, da eben Teile der IP ignoriert werden. Solche mehr oder weniger genauen Auswertungen dürften auf den meisten Webseiten erfolgen – denn u.a. danach wird u.U. die Webseite bezahlt – falls Werbung darauf geschaltet ist.

Greift man auf eine Internet-Seite zu, werden aber auch andere Dinge übermittelt. Dazu gehörten z.B. das Betriebssystem (Mac OS, Windows, iOS, Linux…), der verwendete Browser (InternetExplorer, Firefox, Chrome o.ä.), und die im Browser eingestellte Sprache. Auch die Internetseite, von der man gerade kommt, und sogar die Auflösung des Bildschirms wird u.U. gemeldet bzw. ermittelt. Hier mal eine Seite, auf der einige Dinge angezeigt werden, die beim Surfen im Internet vom Gerät (Computer, Handy u.a.) übermittelt werden. Die Seite ist zwar auf

Englisch – aber was da ausgelesen wird, ist problemlos erkennbar. Hier noch eine andere Variante. Auch beliebt sind verschiedentlich diese Anzeigen auf Webseiten, hier gerade die Daten von Deinem PC:

Abbildung 7: Man kann die angezeigten Werte auch direkt auslesen lassen, ich habe hier mal schnell eine Angebot von www.wieistmeineip.de eingebunden. Im Hintergrund wird also jeder Besuch in diesem Artikel nach dort weitergeleitet und ausgewertet. Die hier angezeigte IP ist (wenn vorhanden) die IP des Routers. Der PC kann eine andere IP haben.

Wozu das Ganze? Zum Beispiel der Darstellung wegen. Vor allem "früher" unterstützten nicht alle Browser alle Funktionen oder Darstellungen einer Webseite. Erkannte die Webseite aber den Browser, konnte die Darstellung angepaßt bzw. korrigiert werden oder der Besucher wurde automatisch umgeleitet. Ein weiterer, aktuellerer Grund: es wird oft unterschieden in eine Darstellung für "richtige" Rechner (Laptop, PC), Tablets und Handys bzw. Smartphones. Für letztere wird das Design wg. des kleineren Displays oft angepasst – auch auf diesen Seiten hier. In vielen Handys bzw. mobilen Browsern kann man einstellen, ob man als "Mobilgerät" identifiziert werden soll oder nicht. Die übermittelte Spracheinstellung kann dafür verwendet werden, die richtige Webseite anzuzeigen, falls sie in mehreren Sprachen vorliegt. Es gibt mittlerweile aber relativ einfache Mittel, so zu tun, als hätte man ein anderes Betriebssystem, eine andere Sprache oder einen anderen Browser – aber darum soll es hier ja nicht gehen…. 🙂

Man sendet aber nicht nur Daten – man empfängt auch Daten. Zum Teil bewußt (z.B. die Internet-Seite mit dem Text und ihren Bildern), z.T. auch unbewußt, z.B. die sogenannten Cookies. Ein normaler Cookie ("Keks") ist eigentlich nichts weiter, als eine Textdatei (Dateiendung .txt), oft mit eingebautem Verfallsdatum. Das heißt: nach Wochen oder Jahren (wirklich Jahre!) werden diese Cookies automatisch vom Browser gelöscht. Man kann Cookies natürlich auch manuell löschen (InternetExplorer: Extras – Browserverlauf löschen, beim Firefox: Extras – Neuste Chronik löschen, unter Details angeben, was gelöschte werden soll……) Man kann die Browser auch so einstellen, das Cookies automatisch täglich gelöscht werden. Übrigens werden diese Cookies auch immer wieder ausgelesen, wenn man im Internet unterwegs ist.

Was machen diese Cookies nun aber? Das ist sehr unterschiedlich. Zum Einen speichern sie, z.T. in verschlüsselter Form, einfach, dass man auf einer bestimmten Webseite war. Sucht man die Webseite ein andermal auf, wird man begrüßt: "Hallo zurück auf unserer Seite" – o.ä. weil anhand des Cookies gemerkt wird: der/die war schon mal hier. Wenn ich nicht irre (das geschieht automatisch durch den Google-Service), wird auf dieser Seite hier anhand von Cookies festgestellt, ob jemand diese Seite zum ersten mal oder zum wiederholten Mal besucht – das wird dann in der Besuchsstatistik ausgewertet: xx % wiederkehrende Besucher, zz % neue Besucher. Oft wird es aber auch für Werbezwecken genutzt: einmal nach einem bestimmten Artikel gesucht? Schon mal vorgekommen, dass danach auf allen möglichen Webseiten Werbung für diesen oder ähnliche Artikel gezeigt wurde? Oder für den zuletzt aufgesuchten Online-Shop? Das kann dann an einem Cookie liegen. Dort könnte gespeichert sein, dass vom gerade benutztem Gerät aus mal nach Artikel XY gesucht wurde. Cookies machen das "Surfen" im Internet also komfortabler – ermöglichen aber auch das Sammeln von Daten (wann und auf welcher Seite war der Nutzer bzw. das Gerät, was hat er gesucht u.v.m.)

Auf einem Rechner sammeln sich aber dutzende, hunderte Cookies – z.T. mehrere je Webseite. Man kann nun dem Browser verbieten, Cookies zu sammeln oder man gibt vor, dass Cookies täglich zu

löschen sind, z.B. beim Starten oder Beenden. Allerdings wird das Surfen u.U. auch komplizierter. Da in Cookies so manches gespeichert ist, muß man das dann immer wieder neu eingeben, wenn man bestimmte Seiten aufsucht, die Cookies aber gelöscht wurden. Mittlerweile gibt es eine neue Cookie-Art, "Super-Cookie", die sich nicht so einfach löschen läßt. Dafür werden aber inzwischen spezielle Erweiterungen für diverse Browser angeboten.

Was also tun?

- immer dran denken: man ist nie wirklich anonym
- man könnte durch diverse Einstellungen falsche Daten senden – sich damit aber auch Probleme (Darstellung der Seiten, Sprache) einhandeln
- möglichst aktuelle Programme (Browser, Mail) verwenden – in alten Versionen klaffen oft Sicherheitslücken
- Tests von Heise prüfen Programme/Router/PC. Hinter den Links sind zunächst die Erläuterungen zum jeweiligen Test. Erst nach klick auf "Der Scan" oder "Test starten" rechts am Rand oder im Extra-Feld im Text startet der eigentliche Vorgang. Evtl. sind rechts noch Unterpunkte auszuwählen.
    - Update-Check prüft Programme auf Aktualität
    - Netzwerkcheck (Router, Firewalls, Ports)
    - Browser-Check Prüft Browser-Einstellungen
    - Emailcheck prüft Email-Program
- Zusätzliche Ad-ons oder Erweiterungen verhindern ungewolltes Übermitteln von Daten, damit könnte z.B. Facebook generell gesperrt werden (auf Seiten mit Twitter-, Google+ – oder Facebook-Button ohne die 2-klick-Variante würde dann auch nichts an diese Unternehmen übertragen) Beispiele sind NoScript (blockiert aktive Inhalte) und Adblock plus (Werbeblocker) die es für verschiedene Browser gibt. Die Einstellung ist u.U. schwierig, zunächst wird fast alles blockiert, dann kann man entscheiden, was zeitweilig oder immer freigegeben wird.
- Wenn man in sozialen Netzwerken ist: öfter mal ausloggen. Daten verschiedener Webseiten nutzen den Firmen vor allem, wenn man sie einer Person zuordnen kann (also demjenigen, der gerade noch bei sozialen Netzwerken eingeloggt ist)
- Öfter die Cookies und anderes löschen. Beim Internet-Explorer: Extras – Browserverlauf löschen, dort dann Auswahl treffen Beim Firefox: Extras – neueste Chronik löschen – dann Auswahl treffen (welcher Zeitraum, welche Bestandteile)

Abbildung 8: Wie man sieht habe ich für die Seite, von der diese Daten stammen, so ziemlich alles erlaubt - hier sind nur noch "verbieten"-Optionen

Hier kurz einige Erläuterungen zum gerade erwähnen Noscript:

Das zeigt mir NoScript auf einer bestimmten Internetseite an, wenn ich in NoScript auf Einstellungen klicke. Ab der 7. Zeile wird es hier interessant – wobei ich mit fbcdn.net nichts anfangen kann. In der 8 Zeile steht dann was von Youtube -was einfach bedeuten kann, dass auf dieser Internetseite ein Video von dort eingebunden ist. Dann folgt schon Google mit Google-Analytics. Dieser auch von mir verwendete Dienst kann o.g. Statistiken für Webseiten erstellen. Contextweb sagt mir jetzt nichts, da müßte ich googeln. WordPress ist eine Software, die solche Blogs wie diesen hier ermöglicht. Die nächsten sagen mir wieder nichts, Gravatar stellt z.B. Grafiken als Benutzerbilder für Kommentare zur Verfügung. Dann kommen wieder Anwendungen von Google, wahrscheinlich etwas, das mit Werbung zu tun hat. Dann kommen wieder einige Dienste bzw. Seiten, die mir erst mal nichts sagen.

Anschließend die “üblichen” Dinge – also Twitter, Flattr, und Facebook. Bedeutet: hier sind die entsprechenden Buttons eingebunden. Flattr ist übrigens ein Dienst, mit dem man gute Webseiten belohnen kann. Mit Klick auf eine Schaltfläche kann man für diese Internetseite Geld vom eigenen Flattr-Konto spenden. Dazu muß Flattr natürlich wissen, wer spenden will – man muß also eingeloggt sein bzw. sich dann einloggen. Flattr müßte also z.B. erlaubt werden.

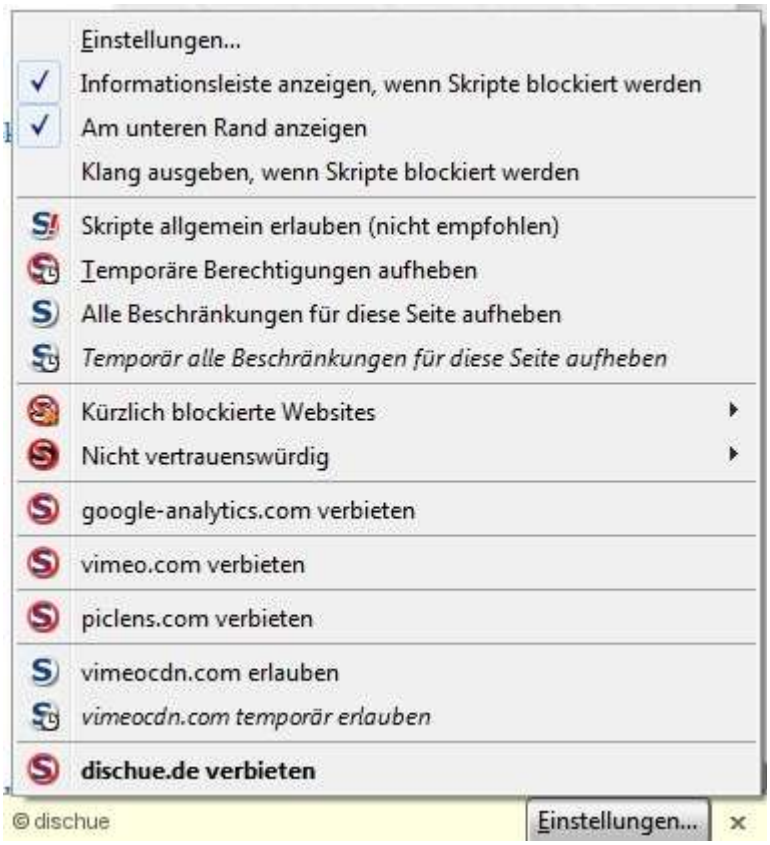


Abbildung 9: Hier kann ich einige Sachen nur noch verbieten, andere müßte ich erst mal erlauben, z.B. vimeocdn - sonst würde ich das Video hier nicht sehen.

Hier mal zum Vergleich die NoScript-Meldungen von einer meiner Seiten.

Die Liste ist wesentlich kürzer. Zum einen, weil ich (noch?) keine Werbung schalten lasse, zum anderen, weil bei mir die Buttons für Facebook, google + , Twitter und Facebook nicht scharf geschaltet sind, da ich diese 2-klick-Methode verwende. Das angezeigte vimeo.com ist übrigens ein Video-Portal ähnlich Youtube aber mit qualitativ höherwertigen Videos – i.d.R. von Profis selbst erstellte Filme. Übrigens ist hier vimeo noch gesperrt, das Video würde nicht angezeigt werden. Erst, wenn ich auf die Zeile *"vimeocdn.com erlauben"* klicke, würde das Video sichtbar. Piclens ist ein Plugin für diesen Blog, der eine andere Betrachtung und Diashow von meinen hier veröffentlichten Fotos ermöglicht.

NoScript blockiert praktisch alle Anwendungen, die nicht von der Seite (hier: dischue.de bzw. Unterseiten) selbst kommen. So kann also das Datensammeln von Facebook, Google usw. verhindert werden. Wenn man merkt, dass etwas auf einer Webseite nicht funktioniert (einloggen, Bestellen, der "Weiter"-Button, der Download usw.) kann man also versuchen, einzelne Sachen in NoScript wieder zuzulassen – temporär oder "immer". Zum reinen Lesen von Text kann meist alles blockiert bleiben…

Wer übrigens noch wissen will, was auf einer Internetseite eigentlich steht, der klicke mal mit Rechts auf eine Freistelle einer Webseite (nicht auf Bilder oder Werbung) und wähle dann "Seitenquelltext anzeigen" oder "Quellcode anzeigen" – aber nicht erschrecken: auf den ersten Blick sehr kryptisch, einige Dinge bekommt man aber heraus. Vor allem wird klar: man kann eine Menge auf einer Webseite unterbringen – ohne, dass der Besucher das merkt.

PC und Internet Teil 4: Datenschutz und online-Fallen 1

Veröffentlicht am 20/02/2012 von dischue

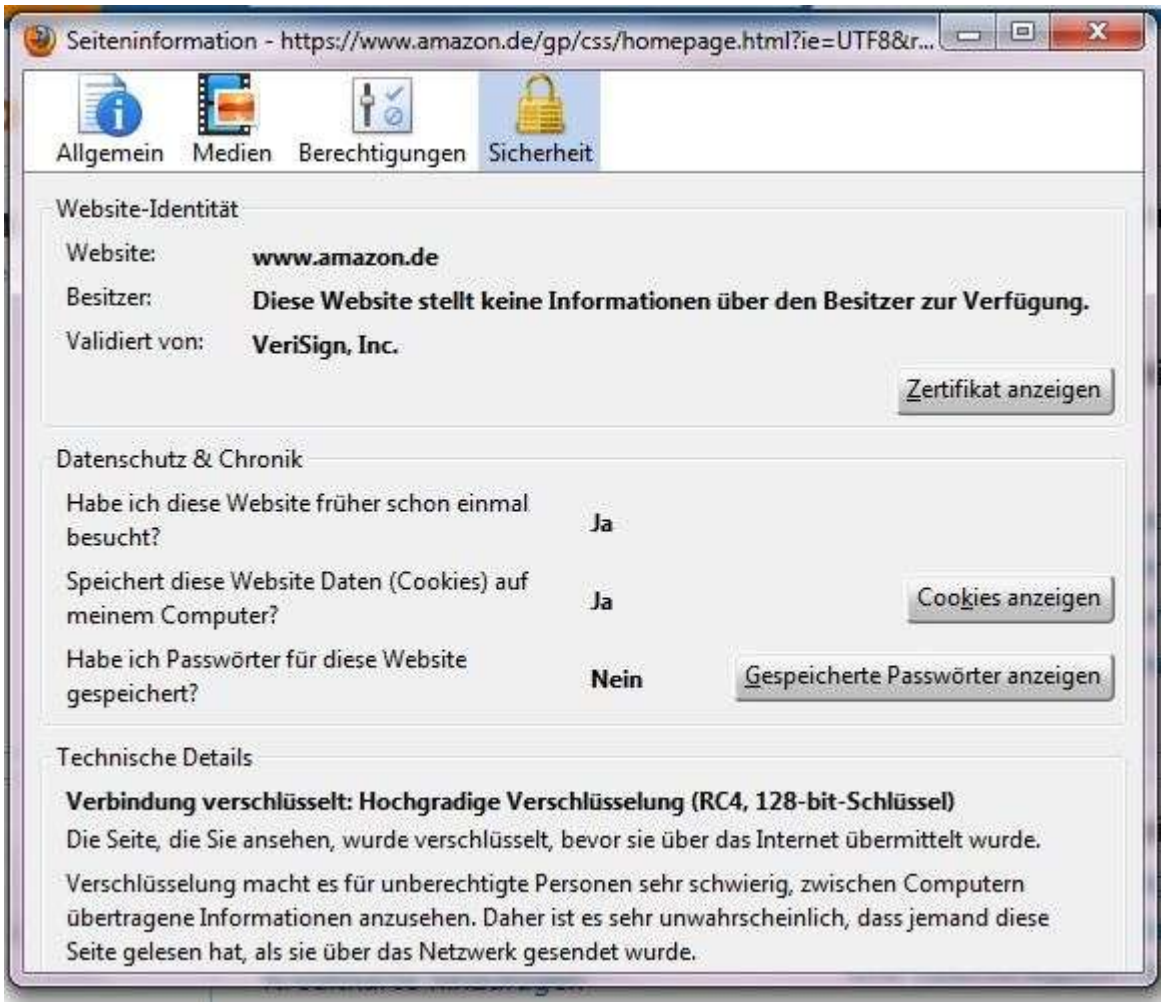
Ging es in dieser kleinen Reihe schon um Datensicherheit, welche Daten im Internet übermittelt werden usw., so soll es jetzt weiter mit dem Thema Datenschutz und Fallen im Internet gehen.

Bei der Datensicherheit ging es ja darum, die Daten vor Beschädigung und Zerstörung zu schützen. Beim Datenschutz geht es nun darum, dass nur der an die Daten herankommt, der das auch soll. Gleich vorneweg: das Windows Passwort ist nicht wirklich ein Beitrag zum Datenschutz. Mit dem Windows-Passwort wird lediglich die Benutzeroberfläche “gesperrt”. Damit hindert man die Kinder kurz daran, eine wichtige Arbeit zu verändern oder zu zerstören oder verhindert, dass Freund/Freundin sehen kann, was man im Internet einkauft. Wer jedoch längere Zeit unbeaufsichtigt auf den PC Zugriff hat, kann recht mühelos alle Daten einsehen und/oder kopieren. Kommt jemand in den Besitz des Computers (z.B. durch Diebstahl oder Fund) ist es überhaupt kein Problem, an die Daten heranzukommen. Übrigens gilt das u.U. auch für gelöschte Daten. Wer seinen PC verkauft oder verschenkt, sollte mehr tun, als nur Daten löschen und Festplatte formatieren. Durch löschen oder formatieren “vernichtete” Daten lassen sich problemlos wieder herstellen. Hier würde nur eine Verschlüsselung der Festplatte helfen oder im Fall des verschenkten Gebraucht-PC das vorherige Überschreiben der Dateien mit unnützen Daten – z.B. mittels Eraser.

Nun aber zum Datenschutz im Internet. Wenn man im Internet einkauft und bei einem online-Shop seine Daten hinterlässt, dann erwartet man, dass dieser Laden die Adresse nicht weiter gibt. Um sich dessen zu vergewissern, kann und sollte man die AGBs lesen (ok, überfliegen) – bevor man seine Daten eingibt. Sollte in den AGBs eine Weitergabe der Daten ausgeschlossen sein, kann man nur hoffen, dass sich der Shop auch wirklich daran hält. Um das dort Gekaufte zu liefern, benötigt der Shop aber nun mal die (Liefer-) Adresse.

Wie erkenne ich denn nun, ob eine Seite seriös ist? Das ist schwer zu sagen. Werbung kann und wird man von fast allen erhalten, bei denen man je gekauft hat. Es gibt natürlich bekannte Anbieter, wie Amazon oder Buch.de – jedenfalls sind diese mir bekannt. Wenn es nach einer Bestellung daran geht, seine Daten einzugeben, wird man zumindest bei den größeren Anbietern feststellen können, dass die Adresszeile statt mit http mit https beginnt – und bei der Eingabemaske für die Daten oft etwas von SSL-verschlüsselt steht. Das s in https steht praktisch für Sicherheit – die Verbindung zwischen dem eigenen Computer und der Internetseite, bei der man bestellt oder ein Forum besucht o.ä. erfolgt dann verschlüsselt. Oft ist dann vor dem https noch ein buntes Symbol, eine Kennzeichnung mit dem Logo der Webseite zu sehen oder irgendwo im Browser das Symbol eines geschlossenen Vorhängeschlosses – alles Anzeichen für eine Verschlüsselung.

Das Unternehmen VeriSign hat in diesem Fall die Echtheit der Webseite bestätigt. Ein klick auf "weitere Informationen" ergibt dann folgende Details:



Einige Antivirenprogramme können auch Webseiten auf ihre Sicherheit überprüfen bzw. erkennen an Hand von White-Lists (weiße Listen – da stehe die "Guten" drin) und Black-Lists (schwarze Listen, da sind die "Bösen" aufgeführt), ob eine Seite gefährlich ist oder nicht. Das können dann aber meist nur die kostenpflichtigen Versionen der Virenscanner. Bei ganz neuen Seiten (dazu im nächsten Beitrag mehr) funktioniert das aber noch nicht – die Seiten müssen ja erst mal als gefährlich gemeldet werden.

Eine weitere Möglichkeit ist WOT (Web Of Thrust – Netz des Vertrauens)- ein Plugin das für die meisten Browser erhältlich ist (auch über die Browser downloadbar). Das funktioniert ähnlich der gerade angesprochenen Virenscanner mittels Listen. Man kann das Plugin ohne Registrierung nutzen – selbst aber nur Seiten melden, wenn man registriert ist. Das soll Mißbrauch verhindern. Das Plugin klinkt sich bereits in die Google-Suche ein und markiert Treffer mit einem roten (gefährlich) gelben (unklar) oder grünen Kreis (ungefährlich). Es gibt dabei mehrere Kategorien (Jugendschutz, Seriosität u.ä.) Da Menschen aus aller Welt beteiligt sind, sind die Ergebnisse aber zum Teil für deutsche Verhältnisse übertrieben streng. So kann eine Seite schon als gefährlich gekennzeichnet sein, wenn dort mal ein Aktbild zu sehen war – und viele Amerikaner o.ä. dies als anstößig empfinden. Zumindest auf deutschen Seiten dürfte das aber kaum vorkommen – denn warum sollten Amerikaner verstärkt auf deutschen Seiten surfen?

Auch der Serverstandort allein (wenn z.B. durch Flagfox angezeigt) ist kein Kriterium für die Seriosität. Viele große Firmen besitzen Server über die ganze Welt verteilt oder stellen ihre Server dort hin, wo es am preiswertesten ist. Man wird dorthin umgeleitet, wo am meisten Ressourcen frei sind. Eine Internetseite mit Endung .de kann also auch in Schweden "liegen". Hier mal das Beispiel von VW:

Abbildung 10: Am Tag, als dieses Bildschirmfoto gemacht wurde, wurde ich auf einen Server in den USA umgeleitet

Ein Mausklick auf die Flagge in der Adresszeile öffnet dann ein Fenster mit einer Übersichtskarte und weiteren Infos:

Eine ungewöhnliche Endung allein oder ein Serverstandort im Ausland sind für sich genommen noch kein Anzeichen für unlautere Methoden oder Absichten. Gefährlich wird es dann, wenn eine Seite versucht, sich als eine andere auszugeben – wie im nächsten Teil dieser Reihe in den Bildern zur angeblichen DHL-Mail ersichtlich. Dort gehe ich dann auch kurz darauf ein, wie man Links so aussehen läßt, als führten sie zur Seite A – man landet dann aber bei Seite B.

Aber es lauern ja noch andere Fallstricke: Freeware. Freeware ist wirklich etwas Tolles – kostenlose Software, die oft wirklich gut ist – Firefox, Thunderbird, OpenOffice, LibreOffice – hier mal einige meiner Lieblingssoftware – größtenteils Freeware. Die Software ist wirklich frei und darf kostenlos verteilt werden. Das Problem: Ganoven nutzen das aus: sie bieten die Software kostenlos an. Man muss aber seine (Post-) Adresse angeben, um zum Download zu gelangen. Irgendwo im Kleingedrucktem steht dann oft was davon, dass man damit ein Abo abschließt – über 1 monatlichen Download oder was auch immer. Seriöse Internetseiten freier Software (Freeware) werden so etwas nicht tun – wie auf den o.g. verlinkten Seiten zu sehen ist – dort müssen keine persönlichen Daten eingegeben werden.

Da wären zum anderen Preisausschreiben…. Es gibt gewiss auch seriöse Anbieter – aber oft geht es nur um das Sammeln von Adressen, an die dann Werbung verschickt wird – das betrifft übrigens auch Preisausschreiben in der Einkaufsstraße, nicht nur im Internet.
Schon mal die Banner auf einer Internetseite gesehen, wo zu sehen ist: *“Sie sind der 1 Millionste Besucher – kein Scherz”* oder *“999999. Besucher”* und dann wird irgendein Preis versprochen. Ich war schon so oft er 999999. Besucher – z.T. immer auf der selben Seite…
Übrigens bedeutet das nicht automatisch, dass die “ganze” Internetseite unseriös ist. Die Werbung wird in der Regel automatisch geschaltet. Vereinfacht läuft das so: ich würde hier einen Platz für Werbung reservieren – habe aber keinen (großen) Einfluss darauf, was für Werbung hier zu sehen sein wird. Es kann sein, dass für eine Automarke geworben wird, für ein Versandhaus oder eben so ein Preisausschreiben eingeblendet wird. Oder aber sich Werbungen abwechseln. Da komme ich aber in einem der nächsten Teil nochmal drauf zurück.

Was also tun?

- immer aufmerksam sein und gesundes Mißtrauen walten lassen
- nicht bei jedem Glücksspiel mitmachen, nicht überall gleich seine Adresse angeben
- auf https bzw. SSl-Verschlüsselung achten – obwohl man sagen muß, das auch kleine Läden ohne https odder SSL seriös sein können – so ein Sicherheitszertifikat ist oft zu teuer
- Im Bekanntenkreis fragen, welche online-Shops sicher sind bzw, wo es Probleme gab oder nicht
- WOT installieren – es ist zumindest ein Indiz, keine Garantie für sichere Seiten.

PC und Internet Teil 5: Datenschutz und online-Fallen 2

Veröffentlicht am 27/02/2012 von dischue

Es gibt jetzt natürlich Überschneidungen mit dem letzten Beitrag…. Ich komme jetzt mal zu bestimmten Mails, die man so erhalten kann. Je mehr man seine (Email-) Adresse im Internet weiter gibt – z.B. über die Preisausschreiben – um so mehr bekommt man auch unerwünschte Post. Auch ohne Weitergabe seiner Mail-Adresse kann man übrigens solche Post erhalten: die Versender dieser unerwünschten Werbung erzeugen einfach zufällig Email-Adressen und schauen, ob die Post ankommt. Das ist so, als würde man Postkarten mit ausgedachten Adressen versenden. Allerdings gibt es bei Emails die Möglichkeit, herauszubekommen, ob die Mail auch ankam – aber das führt hier zu weit. Die Mailprovider und/oder Internet-Provider bemühen sich zwar, unerwünschte Werbemails herauszufiltern – aber das ist ein ständiger Wettlauf zwischen den Spammern und den Providern.

Auf jeden Fall sollte man Mails nie blind vertrauen – selbst dann nicht, wenn sie von einem Bekannten kommen – dessen Rechner könnte infiziert sein oder jemand fälscht dessen Absender-Adresse. Besonders verdächtig sind natürlich Emails, die man erhält, wo aber als Empfänger nicht mal der eigene Name steht. Noch gefährlicher wird es, wenn man in der Mail aufgefordert wird, auf einen Link zu klicken und dort dann seine Anmeldedaten oder was auch immer einzugeben. Dabei wird man meist auf gefälschte oder präparierte Internetseiten gelotst die nur dem Zweck dienen, Daten zu sammeln. Über den letzten bei mir aufgetretenen Fall einer angeblich von DHL stammenden Mail habe ich ja kürzlich hier berichtet.

Hier nochmal der Screenshot der Mails. Zeigt man im Email-Programm oder im Browser mit der Maus auf den Link (Mauszeiger hier nicht sichtbar) sieht man unten links im Email-Programm (oder Browser) wo es wirklich hingeht. (Klappt natürlich nicht bei den Bildern hier)

Die beiden Adressen (Bild oben, eingerahmt) weichen voneinander ab, wie man sieht. Die obere Adresse ist die scheinbare Adresse, auf die man klicken soll. Zeigt man mit der Maus auf diese Adresse, wird unten im Programmfenster (bei Browser oder Emailprogramm) die tatsächliche Adresse angezeigt. In diesem Fall http://packetstation.ro.gp/…. Die Endung .gp bedeutet nun nichts weiter, dass man eine Adresse gewählt hat, die zu Guadeloupe gehört (wie .de zu Deutschland, .fr zu Frankreich oder .pl zu Polen usw.) Das allein ist kein Mangel, selbst für meine Seite hier hätte ich eine andere Top-Level-Domain, also die Landesendung, wählen können. Allerdings legen Firmen aus bzw. für Deutschland normalerweise schon Wert darauf, eine Endung .de in ihrer Adresse zu haben. Verwerflich ist hier, dass man so getäuscht wird – die scheinbare Adresse lautet

ja auf packstation.de. Tatsächlich gelangt man auf diese andere Adresse deren letzter Teil /www.packstation.de/dhl/de/privatkunden/ nun “zufällig” der echten Packstationsadresse von dhl entspricht – hier aber bloß die Namen der Ordner sind, die sich unter http://packetstation.ro.gp/ verbergen – hinter jeden Schrägstrich ein Unterordner des vorigen.

Übrigens wurde die Seite trotzdem in Deutschland gehostet/gespeichert. Wer also Tools wie Flagfox verwendet, sah in der Adressleiste die deutsche Flagge. Allerdings wurde seitens des Hosters wohl schnell bemerkt, dass da was faul ist und die Seite wurde kurz darauf gesperrt. 2 Tage später dann eine ähnliche Mail mit leicht veränderten Details – siehe nächstes Bild:

Letztlich haben sowohl Thunderbird als auch Firefox vor Besuch dieser Seite gewarnt – leider nicht sofort sondern erst einige Stunden nach Erhalt der Email.

Es ist, wie erwähnt, nicht schlimm, einen Link umzubenennen. Das klappt ja auch hier im Text: die Links versuche ich hier so zu benennen, dass sie Bestandteil des Textes sind – zeigt man drauf, sieht man unten links im Browser, wie die richtige Adresse lautet, auf die man geleitet wird.
Kurz gesagt bedeutet das: den Namen eines Links kann ich ganz einfach manipulieren. www.dischue.de muss nicht zu diesem Blog hier führen wenn ich den Link manipuliere. Das Manipulieren geht folgender Maßen:

www.sichtbare Adresse.de

<a href leitet den Code bzw. den Link ein, es folgt (hier rot) die tatsächliche Adresse, auf die man gelangt, wenn man drauf klickt. **target=”_blank”** bedeutet nur, dass für diese Adresse ein neues Browserfenster bzw. -Tab geöffnet wird. Blau ist hier das markiert, was man als Link zu sehen bekommt. **** beendet nur den Code bzw. den Link. Die rote Adresse wird nur unten links im Programmfenster angezeigt, wenn man mit der Maus auf die sichtbare Adresse zeigt (hier funktioniert das nicht, da nur Beispiel). Statt einer sichtbaren Adresse kann man übrigens auch ein Bild nehmen. Diesen und anderen Code einer Internet-Seite sieht man, wenn man mit rechter Maustaste auf eine Internetseite klickt, am besten auf normalen Text oder eine freie Stelle – nicht auf Bildern o.ä. Aus dem sich öffnendem Menü wählt man dann “Quelltext” , “Seitenquelltext” anzeigen o.ä. Eine Manipulation einer Email-Adresse funktioniert übrigens ähnlich – man sieht also eine bestimmte Adresse – sendet aber in Wirklichkeit an eine andere, wenn man nicht aufpasst.

Oft sind solche “falschen” Mails in schlechtem Deutsch verfasst – die oben erwähnte war aber nahezu perfekt, ebenso die Internet-Seite, auf die man geleitet wurde (probiert habe ich das ja…)

Vorsicht auch bei Mails, die eine traurige Geschichte enthalten – ob Krebsleiden oder sonst was. Viele dieser Mails sind seit Jahren im Internet unterwegs und werden immer wieder (neu) weiter gesendet. In der Regel aber nichts anderes als elektronische Kettenbriefe. Gleiches gilt für Mails,

die man an 10, 20 oder sonst wie viel Freunde weiterleiten solle um Glück zu haben, im Lotto zu gewinnen o.ä. Auch, dass Bill Gates Geld verschenkt oder Windows – alles uralte Fälschungen. Es gibt da die scheinbar harmlosen Mails, die irgendwas versprechen, die man nur weiterleiten soll und die Mails, die rührende Geschichten erzählen, von krebskranken Kindern, Menschen die eine Organspende benötigen u.ä. – in der Regel alles Fälschungen – hier findet man eine ungefähre Übersicht über diese sogenannte Hoaxe, die unterwegs sind.

Es gibt auch Mails, die von einem Erbe sprechen – man soll nur z.B. 500 € Verwaltungsgebühr bezahlen o.ä. – Finger weg! Vor kurzem erst eine Mail erhalten, dass eine Namensgleichheit vorliegt und man dadurch an x Millionen Dollar rankommt – ich soll mich erst mal nur melden, ob Interesse besteht – ebenfalls Finger weg!

Ein weiteres leidiges Thema bei Email sind Anhänge. Da kommt eine Email von Max.mustermann@mustermail.de mit dem Betreff "Ihre Rechnung" oder "Mahnung" o.ä.. Aufgeregt, was man denn vergessen haben könnte zu bezahlen, öffnet man die Mail. Darin oft ein Text in der Art: "*Hallo und Danke für Ihren Einkauf, anbei finden Sie die Rechnung. Mit freundlichen Grüßen, Max Mustermann*".

Bevor man jetzt weitermacht, sollte man ganz genau überlegen:

- habe ich jemals bei Max Mustermann eingekauft
- Wie sieht die Abenderadresse aus, für "richtige" Geschäfte wäre eine Mailadresse ähnlich Geschäftsname@mustermail.de oder info@geschäftsname.de üblich.
- Wie sieht die Mail selbst aus? Wird man mit korrektem Namen angeredet? Was soll ich gekauft haben? Ist der Name des Geschäftes ersichtlich? z.B. mit freundlichen Grüßen, Max Musterman, Verkaufsabteilung Geschäftsname. Oft noch eine Impressum mit Umsatzsteuername u.ä.
- was ist im Anhang der Mail? Wenn Rechnungen per Mail versendet werden, dann meist im .pdf Format. Bei einer Datei mit .exe als Endung, z.B. Rechnung.exe, – Finger weg

Folgendes ist nicht als festes Dogma zu verstehen, aufpassen sollte man aber bei:

- Mail oder Webseiten (bzw. Werbebanner), die einen Gewinn, eine Erbschaft o.ä. verheißen
- Emails die zum login und/oder zur Änderung bzw. Überprüfung der eigenen Daten bei Firma xy auffordern und einen entspr. Link bereithalten
- Emails mit rührenden Geschichten oder tollen Versprechungen, die man dafür nur x-mal weiterleiten soll
- Webseiten bzw. Bannern, die behaupten, der Computer sei unsicher – meist wird er es erst, wenn man da drauf klickt
- Vorsicht ist geboten bei Emails, die keine direkte Adresse und/oder keine direkte Anrede enthalten
- Vorsicht auch bei Emails die nicht auf deutsch sind.
- Vorsicht bei angeblich kostenlosen Downloads, bei denen man sein Wohnanschrift angeben soll – oft schließt man hier einen Vertrag über ein Jahresabo o.ä. ab
- Vorsicht auch bei Emails von Bekannten, wenn der Text eher auf gerade gesagtes hindeutet – evtl. weiß der Bekannten nicht mal, dass in seinem Namen Mails verschickt werden.
- keine unbekannten Anhänge öffnen!

Mögliche Gegenmaßnahmen:

- mehrere Email-Adressen; eine mit echtem Namen und andere, "Fake-Adressen" , die man nach gewisser Zeit löschen kann (also nicht für wichtige Sachen wie Steuer, Einkäufe u.ä. verwenden) Kommt dort zu viel dubiose Post an: Adresse löschen lassen. Verschiedenen Anbieter ermöglichen z.B. mehrere Adressen anzulegen (arcor ca. 2, gmx ebenfalls 2, t-online bis zu 10 Adressen in einem Postfach)

- trashmail verwenden
- nicht gleich auf jeden vermeintlichen Gewinn klicken
- nicht bei jedem Gewinnspiel mitmachen
- bei Verwendung eines Email-Clienten (Emailprogramms) wie Thunderbird den Spamfilter aktivieren
- usw…

Und damit kommen wir langsam zu den sogenannten sozialen Netzwerken…. aber das wird dann der nächste Teil dieser Reihe.

PC und Internet Teil 6: soziale Netzwerke

Veröffentlicht am 05/03/2012 von dischue

Immer wieder in den Medien sind die sozialen Netzwerke. Also Google +, Twitter, Studi VZ, Schüler VZ, Stayfriends und viele andere - und natürlich Facebook.

Ein soziales Netzwerk bzw. die Mitgliedschaft ist nicht automatisch schlecht – wie so oft, kommt es darauf an, was man daraus – oder besser damit oder darin macht. "Eigentlich" muß man hier "nur" aufpassen, was man erzählt – und wem man es erzählt. Sicher, das sind "Allgemeinplätze" – aber warum halten sich viele trotzdem nicht daran? Im "realen" Leben würde man seine Adresse nicht einfach einem Fremden geben oder Ihm persönliche Dinge erzählen – also sollte man das in sozialen Netzwerken eben auch nicht tun! Man sollte vielleicht auch nicht rumtönen: ich habe jetzt dieses und jenes Auto, diesen Fernseher und die Stereoanlage – das ist schon fast eine Einladung für Diebe, geradezu ein fertige Liste, was zu holen ist. Selbst wenn auf Facebook und Co eine Adresse nicht öffentlich ist – rauszukriegen ist sie in der Regel trotzdem. Wenn ich in den Urlaub fahre, hänge ich keinen Zettel an den Briefkasten: "Bin gerade nicht da" – also sollte ich das im Internet auch nicht verbreiten.Wenn ich Freunden und Bekannten mitteilen will, dass ich die nächsten Tage nicht da bin, dann kann ich anrufen oder eine Rundmail senden – oder im sozialen Netzwerk nur die informieren, die es angeht… oder doch lieber per Telefon.

Aber warum stehen Facebook und Co immer bzw. des öfteren in der Kritik? Weil man darüber eben nicht nur mit anderen Leuten in Kontakt bleiben kann sondern weil die Daten, Nachrichten die man schreibt u.ä. auch ausgewertet werden – nur weiß man eben nicht genau, wofür, was und wie lange es gespeichert wird. Spektakulär war der Fall eines Studenten aus Österreich: nach mehrmaliger Nachfrage erhielt er eine CD, deren Daten ausgedruckt über 1200 Seiten ergaben – selbst Daten, die er gelöscht zu haben glaubte. Einen groben Überblick bietet auch dieser heise-Artikel. Was machen Facebook oder Google mit den Daten? So genau weiß das eben keiner. Die Daten werden aber z.B. ausgewertet um "persönlich" zugeschnittene Werbung zu versenden. Wer also ständig den "Like"-Button von Facebook benutzt, der bekommt z.B. Werbung von Sachen, die er "liket". Auch meinen Seiten hier kann man Beiträge "liken" bzw. den "empfehlen" Button drücken – allerdings muss man hier erst den kleinen Schalter daneben betätigen, vorher ist der Facebook-Button (bzw. Google+ oder Twitter) inaktiv. Über diese Schaltflächen und das Betätigen derselben können Google und Facebook verfolgen, welche Seiten man besucht. Diese Schaltflächen selbst funktionieren ja nur, wenn man eingeloggt ist bzw. muß man sich dann einloggen. So sehen dann nicht nur die Facebook-Freunde oder die Kreise bei Google+ was man mag oder empfiehlt – sondern auch Google und Facebook selbst. Hat man bei diesen dann noch ein wirklich ausführliches Profil angelegt, kriegen diese Dienste sehr schnell mit, dass sich Max Mustermann aus Musterstadt gern bei Elektronik-Märkten rumtreibt und diese und jene Artikel toll findet und was weiß ich noch alles – solange die bei Facebook gemachten Angaben echt sind.  Selbst bei Leuten, die nicht bei Facebook sind, funktioniert das – nur dass Facebook dann nicht weiß, WER diese Seiten besucht, sondern "nur", von welchem Rechner die Seiten aufgesucht werden. Das sollte aber eben auf meiner Seite hier und auf anderen, bei denen dieser Mechanismus eingesetzt wird, nicht passieren, da diese Buttons erst aktiviert werden, wenn der Schalter daneben betätigt wird. Eine andere Möglichkeit dieses Datensammeln zu verbieten, wäre der Einsatz von NoScript u.ä. Damit sind solche Buttons von Facebook, Twitter, Google.. erst mal völlig wirkungslos, egal wie sie auf der Seite untergebracht sind. Aber dazu in einem nächsten Beitrag mehr. In letzter Zeit ist eine Art Facebook-Trend zu beobachten – oder besser 2:

zum einen reißen die Diskussionen um den Datenschutz nicht ab, zum anderen bitten immer mehr Firmen auf Facebook darum, "geliket" zu werden. Manche Produkte und/oder Sonderaktionen werden nur noch über Facebook angeboten, oft kommt man z.B. nur an eine bestimmte Softwareversion, wenn man auch den "like-"-Button klickt. Manchmal hilft stattdessen auch das

mehrmalige drücken der Tab-Taste (ganz linke Reihe auf der Tastatur, die Taste mit den 2 entgegengesetzten Pfeilen)

Ein anderes Problem der sozialen Netzwerke sind Bestandteile oder Möglichkeiten, "von aussen" bzw. mit anderen Tools darauf zuzugreifen. Erstmal ist das toll: es gibt da eine Facebook-App für iOS, für Android oder sonst was. Es gibt die Möglichkeit, andere Programme oder Dienste damit zu verknüpfen um etwas hochzuladen u.ä. Dazu muß man diesen Diensten den Zugriff auf das jeweilige Soziale Netzwerk einmal erlauben. Die meisten dieser Dienste dürften relativ problemlos sein – geht es oft "nur" darum, auch von Handy aus auf Twitter und Co zuzugreifen. Das Problem ist nur: man verliert den Überblick: 3 Programme probiert – allen mal den Zugriff erlaubt. Dann deinstalliert und vergessen – eine theoretische Zugriffsmöglichkeit könnte aber noch bestehen. Um das zu überprüfen, hat jemand diese kleine Seite gebaut. Die macht im Grunde nichts, als Links anzubieten, mit denen man direkt zu den entsprechenden Einstellungen von Facebook oder Google oder Twitter… kommt. Dort muß man sich evtl. noch mal anmelden und kann dann sehen, welche Programme (auch) Zugriff auf das jeweilige soziale Netz bzw. das eigene Profil in diesem Netz haben. Wenn man sicher ist, dass man das Programm bzw. den Dienst nicht (mehr) verwendet, kann man ihm einfach per klick die Berechtigung entziehen.

Was also tun mit sozialen Netzwerken?

- genau überlegen: brauche ich diese Netzwerke wirklich? wenn ja: welches? Oder genügt z.b. Skype?
- geben ich wirklich alle Daten (wahrheitsgemäß…) an oder lasse ich was weg?
- welche Einstellungsmöglichkeiten habe ich?
- muss ich immer eingeloggt sein oder sollte ich mich öfter mal ausloggen?
- was teile ich über das soziale Netzwerk wem mit? Es soll ja Möglichkeiten geben, dass auch nicht-Mitlgieder bzw. "Nicht-Freunde" z.B. für die Öffentlichkeit gesperrte Bilder trotzdem auf Facebook sehen können und technische Pannen passieren auch immer wieder…
- für o.g. Gewinnspiele oder Sonderaktionen könnte man sich ein Facebook-Konto zulegen, bei dem die persönlichen Daten… nicht so ganz richtig sind…..  klappt natürlich nur, wenn es um herunterladbare Programme o.ä. handelt, nicht, wenn was nach Hause geschickt werden soll. Es gibt für die meisten Zwecke aber sehr gute kostenlose Programme – ohne was "liken" zu müssen.
- öfter mal die Einstellungen und Berechtigungen des jeweiligen Netzwerkes überprüfen

Ob jemand nun solche sozialen Netzwerke nutzt oder nicht, ist letztendlich natürlich Geschmackssache – wenn man sie aber nutzt, sollte man sich genau ansehen, was man einstellen kann, und genau überlegen, was man übers Internet wem mitteilt – und im Zweifel einfach mal nichts mitteilen. Wie im "realen Leben: Reden ist Silber – Schweigen ist Gold…..