(das Internet vor ihnen, oder) Sich und den eigenen PC im Internet schützen

Vorwort

~~Ziel dieses Dokuments ist es, ins kürzester Kürze Sie davon zu überzeugen, dass sie ihren PC (und sich selbst) nicht den Verbrechern im Internet als Fraß vor die Füße werfen sollen.~~ (zu böse)

Wir wollen, **das Internet** besser **vor ihnen** schützen.

Angesprochen sind Laien, blutige Anfänger und sonstige Interessierte.

Tod durch Plastiktüte

Unsere Erfahrung, unser Gefühl vor Gefahren ist für den Schutz unseres Lebens unerläßlich. Dinge, z.B. eine Plastiktüte, können als todbringende Mordwerkzeuge, oder als harmlose Gegenstände angesehen werden. Wie wir damit umgehen, was wir darüber wissen, dass wir verstanden haben, das ist das Wichtigste.

Oft sind wir entsetzt, dass eine Maschine, ein Ding uns doch so gefährlich werden konnte. Und so wird - zurecht - viel Hirnschmalz in die Entwicklung von Dingen gesteckt, dass die davon ausgehenden Gefahren reduziert oder verbannt werden. Dennoch ist noch immer jede Plastiktüte, über den Kopf gestülpt, gut luftdicht am Hals verschlossen nach einer gewissen Zeit tödlich. Man könnte sich wundern, weshalb solche Tüten nicht ohne Notluftversorgung hergestellt werden dürfen.

Auch das derzeit modernste und sicherste Auto ist eine effiziente Tötungsmaschine. Doch Entsetzten über die mangelhafte Technik ist selten zu vernehmen, wenn wieder ein Geisterfahrer auf der Autobahn unterwegs war.

Auf was wir hinaus wollen: Sie müssen den **Computer, das Internet** ein wenig **verstehen**. Ohne dieses Verständnis werden sie immer eine große Bedrohung darstellen. Und auch für sie wird der PC und das Internet eine Bedrohung darstellen. Für beide Seiten, das erklären weiter unten.

Aber nicht nur der Verstand hilf, auch Schutzmittel müssen angewendet (und verstanden!) werden. In unsere Autos haben Airbags, ABS, EPS usw. den Weg gefunden. Dennoch können wir deshalb nicht schneller durch die Kurve fahren und unser Auto merkt auch noch nicht, ob wir versehentlich (oder absichtlich) auf der Autobahn in der falschen Richtung unterwegs sind.

Gefahren im Internet - Die eigentliche Ursache, das Grundproblem

Wir Menschen haben in aller Regel (noch!) kein Gefühl dafür, um *Gutes* von *Schlechtem* rund um den Computer unterscheiden zu können.

Wir sind hilflos, unsicher und leicht auf den Leim zu führen.

Wir besitzen keine natürlichen Sinne um diese Gefahren sehen, riechen/schmecken oder hören oder

erfühlen könnten.

Es wird heiß! Ein Beispiel

Doch ist der Computer da kein Alleinstellungsmerkmal. Welche Sinne haben wir, um uns sicher vor heißen Gegenständen zu schützen? Laden Sie freunde zum Essen ein. Kurz vor dem Essen erhitzen Sie heimlich das Besteck im Backofen auf ca. 200°C und dann flott unbemerkt auf dem Tisch damit. Wer unserer Gäste wird die Gefahr erkennen? Erst im Verlauf des Erwachsenwerdens lernen wir *potentielle Gefahren* frühzeitig zu *erahnen* um dann wie hier *prüfen und einschätzen* zu können:

- Das ist ein Herd - ist die Platte wohl heiss?
- Das ist eine Kartoffel auf einem Teller… heis???!
- Der Käse auf der Pizza…
- Boah… das Lagerfeuer hat die Sohlen meiner Schuhe ruiniert…

~~Schlimmer ist es mit der radioktiven Strahlung, doch auch diese erkennen wir: Wenn wir in ein verstahltes und gesperrtes Gebiet umziehen würden, und dann ein paar Jahre später…~~ (schon wieder, viel zu böse!)

Ok, nein im Ernst: Manchmal helfen nur Messinstromente, Hilfs-O-Meter.

Und am Computer…?

Im Umgang mit dem Computer ist die Sachlage recht traurig: Alltäglich werden wir mit *Schlechtem* konfrontiert, welches wirklich nicht schwer als *schlecht* zu erkennen wäre. Genauso einfach können wir eine heisse Kartoffel ausmachen. Das ist ein Fluch und ein Segen: Noch haben wir sehr gute Chancen uns solide, recht brauchbar zu schützen. Billige Massenangriffe treffen uns tagtäglich. Doch genügend fallen darauf herein. Genauso gut könnten wir über die Erde fiegen und 1 Milliarde Plastiktüten abwerfen. Ich bin mir sicher, einer wird an Erstickungstod durch Plastiktüte über dem Kopf sterben.

Die trickreichen, guten Angriffe erfolgen meist noch gezielt (z.B. Betriebsspionage), dort wo die Täter von den Opfern noch viel mehr erwarten, als sie von uns einzelnen Bürgern erbeuten könnten. Jene Angriffe sind nicht unser Thema. Genauso verlassen wir uns darauf, dass keiner unsere Bremsleitung am Auto angesägt hat. Wir besprechen hier also die „normale“, „alltägliche“ Gefahren und Bedrohungen.

Darum: Wir müssen einzelne Bausteine bei der PC- und Internetnutzung grob verstehen. Haben wir dieses Verständnis, dann müssen wir auch keine Details lernen. Sie bekommen ein Gefühl über die Maschine, genauso wie ein Autofahrer ein Gefühl dafür bekommt, wann er einen Gang hoch- oder runter schalten soll. Menschen sind zu vielem fähig, auch um die Sorgen und Probleme eines Computers verstehen zu können! 🙂

Warum gibt es Viren, SPAM etc. im Internet

Das Internet ist nicht besser oder schlechter als die Menschen es sind. Es ist einfach von Menschen

gemacht. Und hier gibt es eben nicht nur *die Guten*, sondern auch *die Bösen*.

Dennoch ist dies nicht der Grund, weshalb es so viel SPAM, Viren etc. im Internet gibt. Es sind zwei ganz andere Gründe:

- Abertausende, Millionen von Menschen überlassen ihren Computer den Verbrechern als Werkzeug
- Das Internet kennt keine Entfernung im herkömmlichen Sinne: Böse Jungens sind nicht nur in dunklen Gassen zu finden

Natürlich muss man noch weitere Gründe nennen. Zum Beispiel, dass es in der Digitalen Welt (Internet) kein nennenswerten Aufwand bedeutet, ein und die selbe böse Tat noch und nochmals zu verüben/versuchen. Irgendwann trifft der Kriminelle auf einen von dem Personenkreis der „Abertausende, Millionen von Menschen überlassen ihren Computer den Verbrechern als Werkzeug“. Und der zweite oben erwähnte Grund bedeutet nicht nur „die sind überall“, sondern auch „die sind dann auch dort, wo unsere Behörden nichts machen können“.

Ergo: Böse Jungens gibt es immer auf der Welt. Doch Menschen ohne Ahnung und Gefühl für den PC und das Internet überlassen viel zu häufig und fahrlässig ihren Computer den Kriminellen als Werkzeug. Tu was dagegen!

Wie man sich wehrt

Die immer größer werdende Zahl an Menschen, welche sich vom *Überlassen des eigenen PCs an Kriminelle* abwenden, sind sich einig:

- Ich schaue danach, dass alle Programme und das Betriebssystem aktuell sind/bleiben
- Ich habe eine Antivirensoftware (siehe vorheriger Punkt: Aktuell halten!)
- ich habe eine Firewall (was auch immer das ist)

Ein ganz kleiner Kreis dieser Menschen geht noch weiter:

- Ich arbeite nicht als Administrator am PC
- Ich denke nach, ob der Inhalt einer E-Mail, einer Webseite denn nicht eine Falle darstellt, gefälscht ist

Praktisch keiner macht dies:

- Ich ziehe einfache Techniken zu Hilfe, um etwaige Betrugsversuche zu erkennen.

Fazit: Von nun an gehören sie zu dem winzigen Kreis, welcher alle obigen Punkte berücksichtigt - willkommen im Club!

Gegen was man sich nicht, oder nur sehr schwer schützen kann

Hat ein Angreifer physischen Zugriff auf meinen PC (kommt echt da ran), kann jener mich immer überlisten und in den PC einbrechen. Ein PC kann man dagegen nicht schützen. Ach, und der Einbruch

ist sehr einfach und günstig. Für rund 20€ bekommt man in jedem guten Kaufladen entsprechendes Zubehör, echt jetzt. Es geht aber auch ohne Kosten, kommt einfach darauf an, was man mit ihrem PC so vor hat.

Ebenso gibt es immer wieder, tagtäglich neu entdeckte Fehler, Sicherheitslöcher in vielen von den von uns eingesetzten Programmen. Sind diese Fehler noch nicht beim Hersteller, den *Guten* bekannt, sondern eben nur den *Bösen*, dann sieht es potentiell schlecht aus. Darum versucht man *sich von den dunklen Gassen fern zu halten*. Auch bietet man weniger „Angriffsfläche“: Unbenötitge Programme runter vom Rechner. Und eben alles weitere wie oben beschrieben. Um rasch über neue Fehler informiert zu werden, hält man Augen und Ohren offen (dazu gibt es Webseiten, Mailinglisten und Freunde und Kollegen).

Erklärungen zu Warum und Wieso und Wie und Was nicht

Warum man nicht als Administrator am PC zu arbeiten hat

Trifft ein Virus, ein böses Programm auf sie und ihren PC, gelangt an den Schutzmechanismen vorbei (und das passiert definitiv, siehe weiter unten), dann hat es genauso viele Rechte und Möglichkeiten, wie Sie am PC. Sind sie als Administator angemeldet, kann es Dinge am PC verändern, welche sie sich im Traum nicht vorstellen können. Es hat alle Macht „der Welt“. Und es wäre ja **nicht schlimm**, wenn man **nur ihren PC zerstören** und nur **ihr Geld und ihre Kontodaten klauen würde**. Nein, ihr PC ist von nun an meist ein Werkzeug, um andere anzugreifen. Vielen Dank!

Haben sie sich als „normaler Nutzer“ am PC angemeldet, so kann auch Unfug passieren, doch die Hürden für den Missbrauch ihres PCs sind einfach deutlich höher. Wer ein scharfes Messer in der Hand hält, sollte weder sich schubsen lassen, noch unachtsam damit herum fuchteln.

Somit: Als Administrator am PC arbeiten wir also nur, wenn wir ein paar Zwiebeln schneiden müssen!

Virenscanner alleine schützen nicht

Virenscanner wären super, wenn wir erst morgen den PC einschalten würden. Das ist ein zentrales Problem, leider nur nicht das einzige. Dennoch: Viren können von Scannern erst dann erkannt werden, nachdem sich die Viren bereits im Umlauf befinden, von jemandem entdeckt, dann von Experten (und deren Analysesystemen) erkannt wurden, und abschließend ihr Virenscanner hierfür ein entsprechendes Update bekommen hat.

Stand Oktober 2012: Man geht **pro Tag** von rund **einer Million neuer Viren** aus (Schädling versteckt sich hinter der Maus).

Hat man erst einmal einen - guten - Virus und war man auch noch so nachlässig, dass jener mit den Rechnten als Administrator auf ihrem PC arbeiten durfte, kann sich dieser so schützen und verbergen, dass er quasi wie ein HIV Virus ist. Ihr Virenscanner packt so etwas in aller Regel nicht mehr: PC komplett neu formatieren, von Grund auf neu installieren (von einem Fachman!) ist der meist einzige Ausweg.

Fazit

Oft sind die Viren so neu, dass unsere Scanner diese noch nicht kennen können. Virenscanner sind gut gegen „Altbekanntes“, mehr oft nicht.

Firewalls alleine schützen nicht

Ein Spielfilm, durch die Leutsprecher des Fernsehers ertönt: „er hat die Firewall geknackt!“. Doch was für ein Quatsch! Im Alltag müssen die *Bösen* die Firewall meist gar nicht knacken um bei ihnen einzubrechen. Eine Erklärung mit zwei Bildern/Beispielen. Beide hinken, zeigen aber jeweils einen Aspekt (hoffentlich) gut auf.

Ein Bett, ein Haus, ein Feld

Stellen wir unser Bett auf ein Feld. Ohne Wänder drum herum, einfach so. Dann kann jeder der vorbei kommt darauf liegen und auch nachschauen, ob wir frische Bettwäsche aufgezogen haben.

Stellen wir unser Bett auf ein Feld und stülpen ein Haus darüber. Dann ist die Sicht und der „Zugriff“ auf das Haus durch Türe und Fenster beschränkt.

Aber wenn die Türen offen stehen, wenn man durch das Fenster auf das Bett schauen kann, wenn sie die Türe aushängen… nun dann kann man immer noch an ihr Bett, genau so, als stände es ohne Haus da. Welchen Schutz würde uns eine Firewall bringen: Sie würde dafür sorgen, dass die Wände stabil bleiben, damit kein Einbrecher eine neue Türe in die Wand schlägt. Mehr nicht, seltene Ausnahmen gibt es, aber das können wir vernachlässigen. Die Firewall schaut nur, dass die Bahnen der Kommunikation, die Wege, dass jene nicht überschritten oder verlassen werden können.

Ein Telefon zu Hause

Unsere Firewalls zu Hause haben aber noch eine ganz andere Eigenschaft (meist, fast immer). Ich versuche dies mit folgendem Bild zu erklären:

Stellen wir uns unser Telefon zu Hause vor. Es klingelt, jemand ruft uns an. Die Firewall würde dafür sorgen, dass der Anrufer erst mit ihnen sprechen kann, nachdem sie den Hörer abnehmen. Gut. Also genau so wie wir es bisher kennen.

Was solche Firewalls aber praktisch nicht verhindern können: Wenn sie einen Anruf tätigen, wenn der Anruf aus dem Haus kommt, es also ein ausgehender Anruf ist, dann lehnt sich die Firewall zurück und sagt sich: „Das müssen schon sie selber wissen, wen sie anrufen wollen“.

Das bedeutet nun - wieder am PC:

Ist der Virus erst auf dem PC, dann ist die Firewall nahezu nutzlos. Er kann einfach eine Verbindung - egal wohin - in das Internet öffnen. Über diese Verbindung werden dann böse Worte getauscht.

Die erste Erkenntnis: Kommt der *Böse* über die von ihnen erlaubten Türen (sie besuchen einfach eine fremde Webseite - das ist ein Kommunikationsweg), bietet die Firewall keinen Schutz. **Die**

zweite Erkenntnis: Ist der *Böse* erst auf ihrem PC, dann hilft die Firewall selten, da von hier aus dann „nach Draußen“ kein Schutz besteht.

Fazit

Eine Firewall sorgt somit praktisch nur für etwas Ordnung, sie können sich darauf zu konzentrieren, die Türen und Fenster zu pflegen. Durch die Mauer kommt keiner. Unsere Firewalls prüfen also nicht, was oder wer mit uns und unserem PC in Verbindung tritt. Kommt der *Böse* durch die Türe, dann ist das für die Firewall absolut in Ordnung, „so soll es sein“, denkt sich die Firewall. „Alles weitere ist nicht mein Problem“, sagt sich die Firewall.

Hinweis: Es gibt gewisse Modifikationen, weitere Tricks und Kombinationen von Werkzeugen um solche Schwächen abzufangen. So versuchen z.B. moderne Firewalls - kommen wir auf das Telefonbeispiel zurück - sich die Personen ihres Haushalts zu merken („den kenn ich, der darf“, „hu, wer ist den der da? Ich frag mal nach“ *schwupp* ein Windows Fenster erscheint auf ihre PC: „Ein Programm hat versucht… wollen Sie dies zulassen?“) und so weiter.

Software Updates alleine schützen nicht - oder doch?!

Wie wir nun wissen:

Eine Antivirensoftware kann meist nur Böses verhindern, wenn dies „alt“ ist (in Wahrheit: Heuristische Erkennungsmechanismen helfen auch neue, unbekannte Gefahren zu erkennen, doch dies hat auch seine Grenzen).

Eine Firewall kümmert sich praktisch überhaupt nicht darum, ob der Angreifer böse ist. Solange er über die erlaubten Kommunikationswege kommt, ist für die Firewall alles gut.

Was wirklich hilft ist, regelmäßig, täglich den PC, die Programme aktuell zu halten. Sind alle Fehler beseitigt, sind sich unangreifbar (wenn auch sonst nicht's falsch eingestellt wurde). Dieser Zustand ist praktisch aber nicht erreichbar. Das ist reine Theorie. Doch Pflege der Programme wurde im Laufe der Zeit einfacher und einfacher. Mittlerweile bieten alle gängigen Programme eine automatische, eigene Update-Funktion mit. Unser Job ist es, ab und an ein Blick auf die Programmversionen zu werfen. Klappen die Updates noch? Welche Version hat mein Browser, zeigt die Testseite für Java oder Flash an, dass meine Programme auf dem aktuellen Stand sind. (Fachchinesisch, sie wissen sicher nicht, wer denn Flash oder Java ist)

Wenn sie die Nachrichten verfolgen, stellen sie fest, dass wir leider immer wieder tagelang auf Korrekturen, Softwareupdates warten müssen. Die Hersteller kommen nicht immer so schnell voran, wie man es sich gern wünschen würde.

Fazit: Ein fehlerfreier Computer wäre wohl der stärkste Schutz für uns. Diesen Zustand erreichen wir leider nicht, es werden immer wieder neue Fehler entdeckt, neue Programme ersetzten alte und bringen wieder andere/neue Fehler mit.

Der perfekt gepflegte Computer und dennoch geht etwas schief

An verschiedenen Stellen haben wir bereits erwähnt, oder darauf hingedeutet: Wenn sie

Zugangsdaten freiwillig weiter geben, wenn sie den Rechner so einstellen, dass Fremde allerhand Unfug anstellen dürfen, kann sie die Technik nicht schützen. Darum informieren sie sich, fragen sie nach, wenn sie z.B. Skype, E-Mail, Facebook… nutzen wollen. Wenn sie einen Datei- oder Druckserver betreiben wollen, wenn sie Webseiten erstellen wollen. Beachten sie, was ein neues Programm kann, was es unter Umständen Fremden ermöglicht.

Wenn sie keine Experimente starten, dann sind sie keine große Bedrohung für das Internet. Und auch sie werden fast alle bedrohlichen Situationen gut überstehen.

Nicht aufgeben, nicht die Nerven verlieren, Kopf hoch!

Da - wie wir nun endlich wissen - die *Bösen* versuchen, über PCs der *Guten* Unfug zu betreiben, laufen wir eben auch immer Gefahr, uns auf *Guten* Webseiten usw. etwas einzufangen.

Wir können uns nicht immer 100% Schützen: Sie besuchen nur die seriösesten Webseiten der Welt, machen keine unbekannten, fremden E-Mails auf und dennoch schafft es ein Virus auf dem PC, er kam über eine „gute Quelle“ an uns heran. Das kann passieren, wirklich. Doch so what - das bekommt man wieder in den Griff. Viele Jahre können sie aber mit großer Wahrscheinlichkeit problemlos arbeiten, wenn sie es wollen. Und wenn sie von diesem Weg ihre Bekannten und Freunde überzeugen, wir vielleicht einmal in einer besseren Welt leben, dann haben es die *Bösen* auch deutlich schwerer und der SPAM würde nahezu verschwinden…

Beispiele für die Mittäterschaft der Ahnungslosen aus dem Alltag

Angriff über Webserver/Webseiten

Sie mieten „Space“ bei einem „Webhoster“ (will sagen: sie bauen eine eigene Webseite!), sie installieren dort ein Programm, z.B. eine Bildergallerie - egal. Sie machen keine Updates, nichts. Das war's. Nach einiger Zeit wird - das ist 100% sicher - ein Sicherheitsloch, ein Fehler in dieser Software bekannt. Das ist leider so. Immer. Kurze Zeit später wird jemand z.B. ein Programm dort installieren, um SPAM zu verschicken, Kinderpornos zu tauschen, weitere Webseiten installieren, um Kreditkarten abfischen zu können und so weiter und so weiter. Wer war nun schuld?

Darum: Jeder, welcher eine Webseite oder einen PC nutzt, der trägt Verantwortung!

Angriff über E-Mail

Sie erhalten eine E-Mail und werden aufgefordert, ihre Zugangsdaten nochmals auf einer Webseite einzutragen. Das war natürlich die Webseite auf einem (siehe oben) „gehackten“ Webserver, sie wurden herein gelegt.. Kurze Zeit später kann folgendes (oder schlimmeres) passieren: Der *Böse* nuzt ihre Zugangsdaten um SPAM Mails zu verschicken. Leider war das nicht das einzige Problem. Sie haben dabei die Reputation, das Ansehen ihres „Providers“ schwer geschädigt. Universitäten freuen sich immer wieder, wenn der eigentliche Hochschulbetrieb durch den - für die Hochschule weniger lukrativen - Betrieb als SPAM Versender ergänzt wird. In Sekunden bis wenigen Minuten werden die Mailserver der Hochschule von anderen Mailservern auf der Welt blockiert. Zu Recht! Wenn SPAM aus der Hochschule kommt, dann ist die Hochschule ein SPAMmer, dann muss man die Hochschule bekämpfen und blockieren. Dies ist alternativlos für den Rest der Welt. Sie können sich sicher sein,

dass sie eine neue Welle von Aufmerksamkeit in der Hochschule entgegenbraust, sofern es heraus kommt, dass sie es waren (raus kommt das immer, nur gehört es sich, das dann in den betroffenen Kreisen für sich zu behalten. Man muss ihnen dann helfen, dass sie ein zweitesmal nicht in die Falle tappen).

Darum: Jeder, welcher E-Mail nutzt, der trägt Verantwortung!

Dies waren nur zwei sehr populäre Beispiele. Diese treffen recht oft im Alltag auf, sie werden viele Links im Web zu solchen Vorfällen finden.

Fazit - Wie geht es weiter?

Viele von uns haben niemals eine einfache und brauchbare Einweisung und Erklärung für die Nutzung des Internets erhalten. Uns fehlt einfach das Gefühl dafür, welches für Sicherheit und ein behagliches Arbeiten mit dem Computer so notwendig ist.

Das wollen wir in weiteren Artikeln nachholen. Es wird niemals kompliziert. Dennoch: Überaschungen wird es geben, versprochen!

Weitere Artikel mit Basiswissen:

- E-Mail
- das Web

Artikel für aktiven Schutz, ebenso für Laien

- Einstieg in elektronische Signaturen (das ist jetzt etwas weit hergeholt… doch wir haben diese Doku, so sei sie hier verlinkt)