I hob nix g'mocht...

Günter Hartl

Zirp...zirp...zirp...zirp... ein Blick auf das Monochromedisplay meines Nokia 3210 lässt meine ungeschminkte Denkerstirn krausen. Ein Anruf von Gerhard wird am Display artig vermeldet. Nach dem üblichen Small Talk > *"Wo bistn?.am Händi. wüst redn drüber."*, eröffnete er mir, dass er sich wahrscheinlich einen Virus eingefangen hat.

Nach meinen Rückfragen kam es verlegen heraus:

„Äääähh, naja, ich hab mir doch einen neuen PC gekauft, inklusive Microsoft Office 2010. Allerdings nur als 60-Tage-Testversion und ich hatte kein Geld mehr für die Vollversion (oder war zu geizig, eine zu kaufen). Und da dachte ich, da lad ich mir schnell einen Crack runter und spar mir das Geld", vervollständigte ich den Satz. *„Und jetzt passieren auf einmal seltsame Dinge auf Deinem PC, gö?"*

Nach meiner gespielten Entrüstung a la: *„Du willst mich doch nur in den Strudel des Verbrechens reinziehen, da mach ich nicht mit"*, war ich knapp dran, ihn den Microsoft-Schergen auszuliefern.

Da ich aber schon von den James-Bond Filmen her weiß, wie abtrünnige Handlanger behandelt werden (explodierende Bürosessel, Stiegen, die zu Rutschen ins Haifischbecken werden und gnadenlose Hände, die sich in der Waschstraße um meinen unschuldigen Hals legen...nein danke). Da lasse ich meine rechtlichen Bedenken beiseite und mein vegetatives Nervensystem fällt die Entscheidung: Überleben! Also auf zu Gerhard und Windows neu aufsetzen. Aber ohne Crack...

Im Prinzip Alltagskram für mich. Für einen Laien aber ein Horror und undurchführbar. Eine Neuinstallation. Ich weiß schon, dass jetzt wieder die Schlaumeier kommen mit ihrem sagenumwobenen *„wieso, do brauchst doch nur"*. Vergiss das. 70 Prozent der User wissen nicht, wie sie ins BIOS reinkommen. Die anderen 30 Prozent können zumindest die Bootreihenfolge abändern. Der Rest weiß nicht einmal, was das ist. :-)

Zielgruppe auch dieses Artikels sind die Heimuser. Aus einem einfachen Grund. Sie sind nach wie vor die begehrtesten Ziele für Cyberkriminelle *(oiso Verbrecha am Peze, die ihre Webcam immer auf die Seite drehen und nur mit Handschuhen auf der Tastatur herumklimpern > anonüm hoit)*

Meine Zeilen gehen auf die verschiedenen Aspekte von Schadsoftware ein. Es ist definitiv nicht mein Ziel, schadenfroh oder süffisant über Windows7 herzuziehen. Mir geht es eher um die Sensibilisierung der Endanwender bezüglich Schadsoftware und daraus resultierendem Nutzerverhalten. So einen ähnlichen Artikel hab ich vor etlichen Jahren schon publiziert *(wau, tolles Wort)*. Windows XP war damals schwer in Mode. Heutzutage ist es eben Windows7.

Immerhin habe ich ja nach meinem letzten Artikel *„Wos hoitst von dem...?"* erstaunt feststellen müssen, dass meine literarischen Auswürfe doch gelesen werden, bevor sie ihr Gnadenbrot in einem Kanarienvogelkäfig als Kotfänger erhalten.

Danke an dieser Stelle nochmal für die ambivalenten Zuschriften. Ist wenigstens ein bisschen Leben in die Bude gekommen. Oder? Schlecht? Wir wollen ja auch nicht, dass beim Musikantenstadel in den ersten drei Reihen Klatschzombies für Stimmung sorgen müssen *(hüstel.)*.

Back to Topic...

Zuerst einmal, was ist Schadsoftware?

Viren, Würmer, Spyware, Trojaner, Rootkits... Die Unterscheidung ist heutzutage nicht mehr so einfach, weil viele Schadprogramme sich auch „verändern" können. Aber allen ist eines gemeinsam. Es ist Schadsoftware. Oder auch Malware genannt *(Malicious Software)*. *Malicious*=schädlich *(is Englisch, i was)*

Im Artikel werde ich diesen Begriff mit „mw" abkürzen und nicht näher auf die exakte Unterscheidung der Schädlinge eingehen. Die Thematik ist einfach zu komplex.

Wenn Dich das Thema Schadsoftware genauer interessiert, wirf Tante Google an, kauf Dir Fachliteratur und nimm Dir für den Rest des Jahres frei...

Darum kommt in meinem Artikel hier nur das Wichtigste vor.

Für die Erkenntnisresistenten:

- Windows7 > gut
- Malware > schlecht

Das Kochrezept gegen Schadsoftware ist seit XP auch dasselbe geblieben. System aktuell halten, Virenscanner installieren und Hirn einschalten.

Was bei Schädlingsbefall gemacht wird:

Endanwender

Wiederherstellungspunkt, abgesicherter Modus, Recoverypartition einspielen, Reparaturkonsole, Removaltools. daran versucht sich nach einem Supergau der ambitionierte Endanwender. Sinnlos.

Hier noch ein typischer Screenshot von einem Removaltool. Am besten noch mit einem bunten Ampelsystem und alles wird gut. Komischerweise hat es bei mir nie so richtig geklappt...war eher Kosmetik und vor allem... keine Ahnung, was das Tool da auf dem System wirklich gemacht hat (wenn überhaupt)... einfach weiterlesen, unten erläutere ich das noch mit den Removaltools. **(Bild)**

Profi

„Debugging-Tools für Windows"... LiveKD von Mark Russinovich *(warum muss ich bei diesem Namen immer an einen russischen Hacker denken :-))*... sind die Tools der Profis. Damit fuhrwerkt man im Windows-Kernel herum. Ist also nicht ganz trivial und mit einer erheblichen Einarbeitungszeit verbunden. (Sehr gute Kommandozeilenkenntnisse sind unerlässlich)

Im Endeffekt aber als Universallösung bei Virenbefall auch nicht anzuraten, da immer ein Restrisiko besteht.

Die KD-Syntax ist gewöhnungsbedürftig (freundlich ausgedrückt), aber wenn man einmal den Dreh heraußen hat, ist es das mächtigste Werkzeug der Windows-Welt. Okay, falls in meiner Zelle mal der Flachbildfernseher ausfällt... werd' ich's mir vielleicht mal genauer anschauen. Hab' eh schon so viele andere Baustellen offen...

Wenn Du gut bist, ich meine wirklich gut, dann kannst Du mit dem Tool auch Schadsoftware zu Leibe rücken. Ein Restrisiko bleibt aber...

Deshalb auch 2012 mein Tipp bei Schadsoftwarebefall: Neu installieren. Dann gibt's auch kein Restrisiko. Übrigens empfiehlt das auch Microsoft selbst.

Noch einmal in anderen Worten: Das ist wirklich die einzige sichere Methode weltweit, ein schadsoftwarefreies System zu bekommen. (ein sauberes Image geht natürlich auch).

Alles andere ist entweder (noch) zeitaufwändig (er), setzt ein hohes Fachwissen voraus und beinhaltet trotzdem noch immer ein Restrisiko (dass man zum Beispiel nicht sämtliche Schadsoftware gefunden hat...).

Entweder habe ich bisher immer Glück gehabt, oder ich weiß es nicht. Aber letztlich erwischte

es mich doch (oder besser gesagt einen Bekannten und ich durfte helfen…).

Ein Schädling im MBR. Irrigerweise glaubte ich die seit Windows98 für nicht mehr relevant oder zumindest vernachlässigbar. Irrtum.

Obwohl die Kiste während der Installation noch nie Kontakt mit dem Internet hatte, meldete sich der Schädling eifrig zu Wort. *What the FU… „Das gibts doch nicht“*, dachte ich noch. Dann dämmerte es mir. Da ich die Festplatte bei einer Neuinstallation immer formatiere (nicht lachen, das ist nicht selbstverständlich bei vielen Usern), blieb logischerweise nur mehr der MBR als Fehlerquelle über.

Der MBR *(Master Boot Record)* ist der erste Datenblock auf einem Speichermedium. Da er „nur“ 512 Mbyte groß ist, kann er nur beschränkt große Informationen drin halten (Partitionstabelle, Info zu Bootloadern.). Darum gibt es ja auch die Partitionsbeschränkungen auf jeder Festplatte. Maximal 4 primäre bei IDE-Platten. Weil einfach nicht mehr Platz für weitere Informationen ist.

Ebenso der Hauptgrund, warum Schädlinge möglichst „klein“ entwickelt werden. Im MBR haben sie dann Platz und können dann ihrer zugewiesenen Aufgabe entsprechend weitere Komponenten übers Internet nachladen. Keine Angst, das Ding wird schon „größer“ und es werden immer - ich betone **immer** - Komponenten nachgeladen.

Ergo: Wenn Du neu installierst, musst Du auch immer den MBR löschen (oder überschreiben)

Problem: für „normale“ Endanwender: unmöglich, das zu bewerkstelligen.

Falls Du ein Imageprogramm hast, das auch den MBR mitsichert… no Problem. Erkundige Dich diesbezüglich vorher, ob das bei Deinem Imageprogramm so ist. Du hast doch eine Image-Sicherung, oder…?

Da die meisten so was eben nicht haben, wird‘s immer zeitaufwändig. Keine Festplattenunterteilung in „C“ und „D“ oder sowas in der Richtung heißt, Daten sichern vor dem Formatieren. Kann schon dauern…

Der Endanwender sitzt mit fragenden Augen daneben und murmelt nur irgendwas von *„dos des so fü Orbeit is, hätt i net docht.nur wegn dem an Virus“.*

Heißt: Den meisten ist noch nicht mal ansatzweise die Tragweite der Infizierung bewusst. Google mit seinen Removaltools sorgt schon dafür, dass die Urlaubsfotos nicht verloren sind. Wer‘s glaubt…

Willst Du einem Otto Normalverbraucher wirklich zumuten, dass der ellenlange Logfiles von „malwarebytes“ in Foren postet und mit den darauf empfohlenen Schutzprogrammen auf Schädlingsjagd geht?

Da sitzen Endanwender, die großteils nicht mal den Unterschied zwischen Kopieren und Verschieben kennen. *(„wozu auch.i moch des imma so“)*.

Was soll der mit einer Software, die im Admin-Modus an seinen Systemfiles herumtut?

Bleib‘ am Boden. Neuinstallation. Oder richte ihm wenigstens ein Image ein. Alleine schon der Zeitersparnis wegen.

Wer den MBR löschen will (muss), kann das mit einer Linux-Live-CD machen. Wenn ich die Vorgehensweise jetzt hier auch noch detailliert beschreibe, dreht mir der Franz (mein Chefredakteur) noch durch und baut mir meine Tastatur aus…

Hier ein brauchbarer Link, der das Szenario schrittweise für Anfänger erklärt. Sehr hilfreich.

http://forum.chip.de/viren-trojaner-wuermer/faq-thinkpoint-entfernen-1443209-page2.html#post8738501

Userreaktionen bei Malwarebefall

Der Schock sitzt bei vielen Usern tief. Egal, wo sie auch nachfragen, es läuft immer auf eine Neuinstallation hinaus. Sprich, ein paar Stunden Arbeit. *„Gibts do ka afochare Möglichkeit?“ „Nein, außer Du hast ein sauberes Imätsch“. „Wos is a Imä… vergiss es. Neuinstallation“.*

So ungefähr läuft der Dialog ab. Ab hier wird‘s spannend. Manche lehnen das kategorisch ab, weil sie glauben, dass es sich der Helfer leicht machen will. Foren werden bemüht. in der Hoffnung, eine „zeitsparendere“ Lösung angeboten zu bekommen.

Dabei ist das Neuaufsetzen wesentlich aufwändiger als das Löschen einzelner Dateien. Das Löschen einzelner Dateien entfernt jedoch nur die Symptome und ist keine brauchbare Lösung.

Natürlich gibt es genug Endanwender, die entrüstet diese drastische Maßnahme überhaupt nicht zulassen wollen und darauf beharren, dass es da „eine leichtere Lösung“ geben muss. Die gibt es allerdings. Hab sogar schon ein paarmal erlebt, dass sich Betroffene einen neuen PC gekauft haben, weil sie nicht „so viel Zeit für die Reparatur haben und Arbeiten müssen“.

Auch wenn jetzt viele mit den Augen rollen werden. Das ist die Wirklichkeit. Das ist das Leben…

Das gibt es öfters, als Du glaubst. Üblicherweise wird nach dem Malwarebefall noch zwei bis drei Wochen weitergearbeitet (keine Ahnung, wie man mit so was noch vernünftig arbeiten kann) um dann entnervt den nächsten Media-Markt zu stürmen und einen PC zu ordern. 5 Tage warten auf die Reparatur? Nein! Und während der drei Wochen haben sie schon wieder zig andere Rechner infiziert…

Speziell wenn die Leute noch an einem Projekt arbeiten und die Deadline einhalten wollen… oder es *"gerade jetzt ungünstig ist, neu zu installieren."*.

Bedenke noch mal. Das sind großteils Endanwender. Beim Auto brauchst ja auch nur den Keilriemen tauschen und das Werkl rennt wieder. Wer tauscht da schon den ganzen Motor?

Welcher PC muss jedes Jahr zum „Pickerl“… welcher Endanwender hat einen PC-Führerschein? Siehst Du, worauf ich hinaus will?

Der PC ist kein Toaster, den man einschaltet und gut ist‘s. Ich kenne noch immer Leute, die sich über die 30-sekündige Startzeit aufregen, weil ja jeder Elektromotor auf Knopfdruck „anspringt“.

„Gibts do kane Remufltuls?“. Schon, aber vergiss das.

Removaltools

Mit Removal-Tool bezeichnet man Programme, die den Anspruch erheben, einen infizierten Computer vom Schädling zu bereinigen, ohne dabei eine Neuinstallation nötig zu machen.

Darunter fallen sowohl die Desinfektions-Routinen von Antivirenprogrammen wie auch die speziell für bestimmte Schädlinge entwickelten Entfernungsprogramme. Exemplarisch sei hier McAfee AVERT Stinger erwähnt, obwohl das Gesagte für alle anderen ebenso gilt.

Die meisten Removal-Tools werden direkt auf dem befallenen System benutzt. *No na.* Man hat einen infizierten PC, lädt sich irgendein Tool zum Entfernen herunter und startet es. Das klappt so nicht. Abgesehen davon, dass das Herunterladen von Rettungstools auf einem kompromittierten System meist sowieso nicht gelingt. Die Schadsoftwareerzeuger verstehen ihr Handwerk… die meisten halt. Oder sagen wir so: Schadsoftware gehört mitunter zu den ausgereiftesten Produkten im IT-Feld. Wenn ein Schädling nicht das komplette System befällt, sondern zum Beispiel nur Dein Benutzerkonto, dann muss er schon ziemlich „schlecht programmiert“ sein.

Das System wurde ja bereits infiziert. Der Schädling (bzw. der Angreifer, der über den Schädling den Rechner kontrolliert) kann Teile des Systems ausgetauscht oder manipuliert haben.

Merke: wenn Du keine Kontrolle mehr über das System hast, hast Du keine Kontrolle mehr über das System.

Nochmal: wenn Du keine Kontrolle mehr über das System hast, hast Du keine Kontrolle mehr über das System.

Wieso solltest Du keine Kontrolle mehr über das System haben?

Ein aktiver Schädling übernimmt immer die Kontrolle über das System. Man nennt das auch *„Kompromittierung des Systems“*. Sprich: Keiner weiß genau, was da jetzt auf dem System „passiert“. Es gibt mitunter Hunderte verschiedene Varianten einzelner Schädlingen. Ein aktiver Schädling auf dem System reicht. Ehrlich. Auch wenn weiterhin der Explorer normal funktioniert.

Und nein, da poppen keine lustigen Fenster auf mit *„Ätsch.Virus“*, oder es wird eine lustige Musik abgespielt. Das funktioniert maximal in Konfetti-TV so.

Das Removaltool arbeitet immer mit den Funktionen des Betriebssystemes. Anders geht‘s nicht. Wenn diese Funktionen aber so manipuliert worden sind, dass das Betriebssystem das Tool anlügt, kann das Tool gar nicht funktionieren. Sehr beliebt ist auch noch die Erfolgsmeldung des Removaltools abzuwarten und durchzuatmen. Selbst wenn Du den Schädling entfernt haben solltest…äääähhh, die Meldung kam vom kompromittierten System.

Das Problem ist ja nie (oder selten) die gefundene Schadsoftware. Sondern immer: was hat der in der Zwischenzeit gemacht?

Fazit: Keiner will einsehen, dass wegen so einem blöden Trojaner oder Wurm gleich der ganze PC im Eimer ist und die Festplatte formatiert werden muss.

Hier nochmal der wichtigste Grund, der alle anderen Einwände schon obsolet macht. Du arbeitest immer auf einem nicht vertrauenswürdigen System.

Was machst du noch da? Vergiss es, gib das System auf und schau, dass der Schaden nicht grösser wird. Schadensbegrenzung eben.

Sobald eine Schadsoftware auf dem System installiert wurde…

1. tritt sie Systemprozessen und Systemprogrammen bei und manipuliert dessen Verhalten. Üblicherweise die Suchfunktion und Anzeige von Dateien, sodass ihre eigenen Komponenten nicht aufscheinen.
2. Deaktiviert und (oder) manipuliert sie alles, was sie an „Schutzprogrammen“ findet (Hintergrundwächter…)

Sie legt an verschiedenen Orten Kopien unter verschiedenen Namen ab. Diese Namen täuschen dann harmlose Dateien oder unentbehrliche Systemdateien vor, an die sich allein des Namens wegen der Benutzer nicht herantraut, selbst wenn er auf sie aufmerksam wird.

3. verhindert sie den Zugriff auf Systemprogramme wie den Task-Manager oder die Registry (in Windows), so dass der User keinen Zugang zum System mehr hat. Malware manipuliert die Registrierdatenbank von Windows (Registry) so, dass Kopien ihrer selbst zuverlässig auf die eine oder andere Art und Weise beim Neustart automatisch mitstarten.
4. Malware „kennt“ die Standardordner und Dateien, in denen Passwörter und vertrauliche Informationen über den Anwender abgelegt sind, liest diese aus, entschlüsselt sie und speichert sie in einem eigenen Logfile zwecks späterer Verwendung und Verbreitung via Internet
5. Malware sammelt Mailadressen, die es im Mailprogramm, in Seiten des Browsercaches und dem Verlauf (History) und anderen Dokumenten findet. Mit diesen gültigen Adressen erzeugt sie zusätzliche Adressen auf gut Glück, die aus den Bestandteilen der existierenden zusammengewürfelt werden. Auch hiervon wird eine Liste angelegt.
6. Malware öffnet eine Hintertür ins System, über die ein Fremder mit dem passenden Gegenstück dieser Software (dem Client) - die Malware ist in diesem Fall der Server - den Rechner live via Internet praktisch beliebig fernsteuern kann.
7. lädt sie aus dem Internet weitere Schadsoftware nach, die wieder andere Fähigkeiten und Aufgaben übernimmt. (Passwörter auslesen, Spielstände, Lizenzkeys, Kontodaten, Spamverteiler und eigenes Dateisystem einrichten, Anschluss an Botnetz…)
8. Malware besitzt ein eigenes Mailprogramm oder nutzt das des Benutzers und verschickt sich selbst, die vorgenannten Listen und private Dateien unbemerkt an andere Rechner oder als Spam-Bot automatische Werbemails.
9. kann sie den Internetzugang kontrollieren und verhindern, dass man die Seiten von Virenscanner-Herstellern aufruft. Ditto bei Windows-Updates oder Aktualisierungen der Virenscanner.usw.

Malware arbeitet extrem unauffällig und raffiniert im Hintergrund und zielt nicht primär auf Datenzerstörung sondern auf Spionage und Missbrauch ab.

Noch einmal, wir schreiben das Jahr 2012, und nicht 2003, wo man mit XP und der ausufernden Schadsoftwaresituation damals erst so richtig ins Bewusstsein der Leute vordrang.

Die oben erwähnten Punkte sind seit Jahren gängige Praxis und werden kontinuierlich weiterentwickelt. Vor allem in Bezug auf neue Betriebssysteme und Virenscanner.

„Oba i hob ollas skänt und er hot nix gfundn“, wie oft hab ich das schon gehört. Noch einmal, die Aussagekraft eines lokalen Virenscanners geht immer gegen Null. Ist so. Der Virenscanner ist Teil des kompromittierten Systems…

Du müsstest immer von einer *„garantiert virenfreien“* Systemumgebung scannen. Am bekanntesten sind Antivirus-Boot-CDs. Kaspersky mit seiner Rescue-Disk zum Beispiel. Läuft auf Gentoo-Linux. Mit dem könntest Du Dein System säubern, ja. Aber auch da hast Du ein Restrisiko.

Egal, ob Du Dich mit einer Rescue-Disk, Cleaningtools oder manuell an die Beseitigung des Schädlings heranmachst. Im Endeffekt kann das System wieder „sauber“ sein. Muss aber nicht.

Bei einer Neuinstallation (oder dem Einspielen eines sauberen Images) ist das System immer in einem „sauberen“ Zustand. Das funktioniert immer.

Nachteil: Zeit-und Nervenaufwand…

Uninteressant für Heimanwender. *„wie bekomm‘ ich das iso-file auf die CD oder gar auf einen USB-Stick.?“… „was ist überhaupt ein iso-file?“ „und dann?“.*

Da müsste man schon ein bisschen Zeit investieren, um damit sinnvoll arbeiten zu können. Aber auch hier bleibt das altbekannte Restrisiko bestehen…

Am Seitenende sind ein paar nette Schnappschüsse von „falschen“ Schutzprogrammen, die per Malware ins System geschleust wurden. Gibt‘s natürlich in allen Ausprägungen und Sprachen…

Für was ein Virenscanner dann gut ist? Meiner Meinung nach sollte der „anschlagen”, wenn mw mit Deinem System in „Berührung“ kommt. Da ist das Kind noch nicht in den Brunnen gefallen.

Außerdem ist ein Virenscanner nur ein Teil von einem Sicherheitskonzept und vor allem nicht der „entscheidende”, wie es gerne suggeriert wird.

Wenn ein Virenscanner zum Beispiel meldet, dass die `explorer.exe` (oder eine andere Datei) diese oder jene mw enthält, dann ist es auch relativ sinnfrei, diese Datei zu löschen, oder durch ein Original von der Windows-Installations-CD zu ersetzen. Großteils bezieht sich dieser Fund auf die Kopie der Datei. Und die liegt im Arbeitsspeicher. Ergo, ist diese Aktion wirkungslos.

Zusätzlich installiert Malware üblicherweise Komponenten, die selbige überwachen. Falls diese zufällig doch gefunden werden sollte und aus dem Arbeitsspeicher oder der Festplatte entfernt werden sollte, wird sie sogleich ersetzt. Dabei ist es unerheblich, ob das Löschen des Schädlings manuell oder per „Schutzprogrammen“ erfolgt ist.

All dies ändert aber nichts an der Ursache der Infektion: Entweder war das System nicht aktuell (muss nicht unbedingt Windows oder der Virenscanner sein) oder der User hat eine Interaktion (klick…) ausgeführt. Somit sind neue Infektionen vorprogrammiert.

Verschärft wird das Dilemma noch durch den Umstand, dass eine installierte Malware immer weitere Komponenten aus dem Internet nachlädt. Sie holt praktisch immer Verstärkung. Diese Verstärkung ihrerseits macht was? Genau, die holt wieder andere Komponenten aus dem Internet nach, wenn nötig spielen sie gegenseitig Updates für die Malware ein, deinstallieren (bekannte, schlecht programmierte) Malware und nisten sich im System ein.

Dämmert‘s schon? Während Du noch siegestrunken mit einem Removaltool die `setup.exe` niederklickst und den Übeltäter im digitalen Nirwana wähnst, haben seine Kollegen schon ganze Arbeit geleistet. Artig meldet das Tool die Entfernung der Malware und alles ist ruhig. Einmal kurz ausatmen und den vermeintlich todsicheren Tipp gleich prophylaktisch seinem besten Freund mitteilen. Der PC verhält sich normal, noch schnell in den Taskmanager geschaut. alles okay. Vergiss es. Wie willst Du etwas überprüfen, das Du nicht siehst?

Sobald einmal Schadsoftware aktiv war am System, hast Du keine Kontrolle mehr über dieses. Na klar fällt Dir nix auf. Ziel erreicht…für die andere Seite.

Ich weiß schon, dass der alleinige Gedanke einer Neuinstallation der blanke Horror ist. Für Profis und Anfänger gleichermaßen. Erstere gehen im Kopf schon ihre Checkliste durch (Treiberquellen, Installations-CDs, Lizenzkeys, Outlooksicherung, Skype-Kontakte, Autocadmonster installieren, Updates und gesicherte Daten einspielen… *„wo san meine Läsezeichn?“*.man geht auf jeden Fall spät schlafen). Letztere schaffen's meist innerhalb einer Woche, ihr System halbwegs brauchbar wieder herzurichten; wenn überhaupt.

Wenn Du die Geschichte zu Ende denkst, und es schön langsam vom Hals aufwärts warm wird, tja… wenn es nur ein lokales Problem wäre. Aber dank Breitbandanschluss wird man natürlich andere Rechner genauso infizieren oder (und) mit Spam belästigen.

Beispiel Suche XP Antispyware

Im Security Center sollte eigentlich alles grün sein

Was machen die Provider, wenn sie merken, dass Du eine Spamschleuder bist? Genau, die drehen Dir die Leitung ab, bis Du Dein System wieder in Ordnung gebracht hast. Vor allem bei Privatusern…schon oft erlebt. Ja, auch bei Windows7. Eigentlich sollte er froh sein, dass ihn sein Provider darauf „aufmerksam“ macht.

Es hilft alles nix. Das beste (und einzig sichere) Mittel bei Befall von Schadsoftware > Neuinstallation. Gilt immer noch, auch für 2012.

Verhalten von Opfern.

Meiner Meinung nach gibt es bei mw-Infektionen 2 Gruppen von Opfern:

1. Leute, die dazulernen
2. Leute, die aufgebracht nach neuen Gesetzen und Strafverfolgung schreien, aber nicht ihr eigenes Verhalten hinterfragen.

Die zweite Gruppe ist eindeutig in der Überzahl. Deshalb gibt es auch so viel erfolgreiche Schadsoftware.

Vor allem verstehen viele Betroffene nicht einmal ansatzweise, was die „Hacker“ überhaupt auf seinem PC suchen oder was sie erreichen, wenn sie sich Zugriff verschaffen.

Es fehlt jegliche Einsicht, dass Daten, die ausspioniert werden, bares Geld wert sind - egal ob nun so bekannte Dinge wie Kontodaten und Passwörter oder weniger offensichtliche wie Registrierungs-Keys, E-Mail-Adressen oder Spielstände . Jede gestohlene Information lässt sich zu Geld machen. Jede.

Weiterhin wissen viele nicht, dass ihr PC ferngesteuert andere Rechner weltweit infizieren, mit Spam-Mails überschütten oder illegale Transaktionen verschleiern kann. Und selbst wenn sie es wissen, kommt als Reaktion oft so etwas wie *„Wos gät des mi an?“*

Sehr viel. Wenn Du Spam in Deinem Postfach hast, heißt das nichts anderes, dass zumindest einer (oder eher viele) auf diesem Planeten genauso denken… und auf einer Spamschleuder arbeiten.

Und ich kenne keinen einzigen mit Email-Adresse, der nicht schon mal ein Spamproblem hatte. Somit sind heutzutage Spamfilter (oder aufwändigere Einrichtungen und Technologien zur Vermeidung von Spam) unerlässlich. Selbst wenn Du heutzutage keine Spam bekommst, hat die Drecksarbeit der Spamfilterung eben Dein Provider übernommen. Keine Angst, der verrechnet Dir das sowieso (und uns auch). Über die monatlichen Gebühren. Du siehst also, wohin das führt…

Wer macht so was und warum?

Der verhaltensgestörte Einzelgänger in seinem Kämmerlein war einmal. Heutzutage hat man es immer mit professionell organisierten Kriminellen zu tun.

Nach Ruhm und Ehre in der Hackerszene zu streben? Welche Filme schaust Du Dir eigentlich an? Das ist Hollywood. Heute geht‘s nur mehr um drei Sachen. Money, Geld, Kohle.

Nenn‘ es, wie Du willst. Oder kennst Du wen, der gratis arbeiten geht? Oder meinetwegen aus Spaß? Eben. Alle „erwarten“ am Siebenten ihre Kohle am Konto. Nur gehört es bei uns nicht zum „guten Ton”, so was auch nur anzudenken. (für Geld zu arbeiten).

Selbst wenn es zu wenig Geld ist, wird deshalb immer gleich der prophylaktische Entwaffnungssatz *„mir mocht die Arbeit aber Spaß“* nachgeschoben. Das „aber“ ist das Problem.

Bei den Kriminellen nicht anders. Glaubst Du wirklich, die geben sich mit einem achtungsvollen Schulterklopfer zufrieden? Oder mit dem Titel *„Hacker des Jahres“*? Denk' nach.

Kriminelle machen aber nur dann Gewinn, wenn ihre Schadsoftware erfolgreich ist und so lange wie möglich unbehelligt arbeiten kann. Deshalb gibt es auch so viele Updates… für die Schadsoftware selber… Ja, auch die Malware wird upgedatet, kein Spaß.

Daraus kannst Du schließen, dass es im ureigensten Interesse der Kriminellen ist, absolut professionelle Schadsoftware so schnell und flexibel wie möglich in Umlauf zu bringen.

Dafür brauchen die nicht einmal ein Call-Center für die Abwicklung des Supports, Angestellte oder großes Startkapital.

Schutzprogramme

Dem gegenüber haben wir die Hersteller von „Schutzprogrammen“. Mittlerweile eine Milliardenindustrie. Natürlich arbeiten die auch gewinnorientiert. So wie jede Fluglinie auch, obwohl deren Pressesprecher mit seriösem Augenaufschlag sein indoktriniertes *"Sicherheit hat bei uns oberste Priorität"* loswerden muss. Wenn's so wäre, gäbe es schon lange (wie beim Militär) Sprinkleranlagen in Fliegern.

Der Gewinn der „Schutzprogramm“-Hersteller beruht jedoch auf Angst, dem Marketingerfolg und der Un(wissen)sicherheit der Kunden. Daher ist es auch im Gegensatz zu den Kriminellen nicht unbedingt „nötig”, perfekte Software zu entwickeln.

Ängstliche Menschen, die das Zeug kaufen, das brauchen sie. Den „ängstlichsten“ User erkennst Du leicht. Der hat immer den teuersten Virenscanner. Freeware-Virenscanner *„san nie so guad“* und absolutes Tabu.

Der beste Virenscanner befindet sich meiner Meinung nach noch immer zwischen den Ohren.

Erschwerend kommt hinzu, dass diese Unternehmen in erster Linie dem Aufsichtsrat und Aktionären verpflichtet sind. Das heißt, Management und mangelndes Interesse beeinflussen die Softwareentwicklung der Schutzprogramme.

Fazit: Eine Software oder Behörde „kann“ keine Abhilfe schaffen.

Das einzige, was die Kriminellen brauchen: veraltete, fehlerhafte Software bei ihren Opfern, gepaart mit deren Leichtgläubigkeit und Unwissenheit.

Wenn das gegeben ist, kommen enorme Gewinne zustande (Daten von Trend Micro)

Gewinne

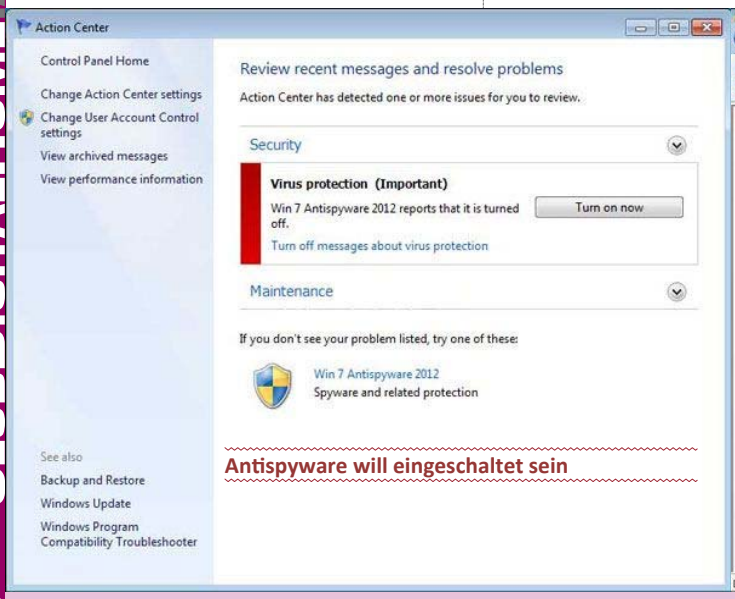
- 1-3 $ pro US-Kreditkarten-Nummer
- 3-8 $ pro Kredikarten-Nr. anderer Industriestaaten in Mittelamerika, Australien oder Europa
- 6-10 $ pro Kredikarten-Nr. anderer Länder z.B. in Asien oder im Mittleren Osten
- 25-35 $ pro Satz von Bankkonto-Anmeldeinformationen
- 15 $ für 1000 Facebook-Account-Zugangsdaten
- 75 $ für 2200 Twitter-Account-Zugangsdaten
- 8 $ für 1000 Hotmail- oder Yahoo! Mail-Zugangsdaten
- 85 $ für 2500 Gmail-Zugangsdaten

Und da sind noch nicht mal die Preise für‘s Hosten, Lizenzkeys, Skype…dabei.

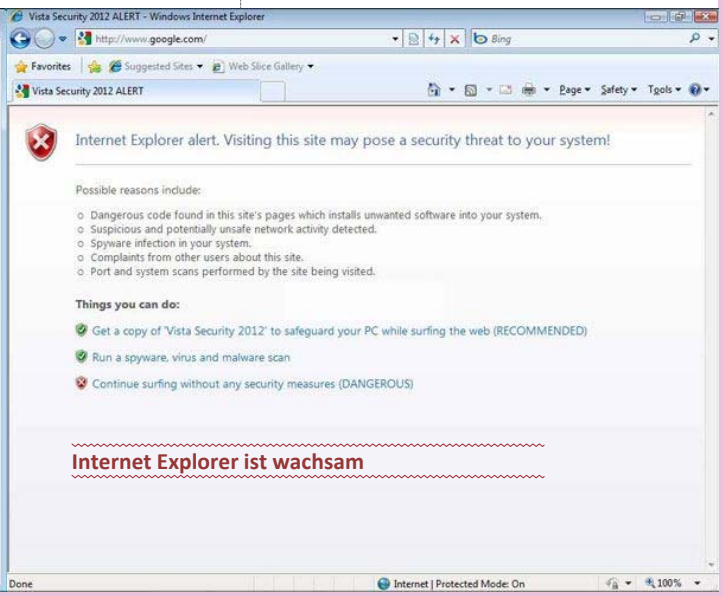
Stell‘ dir vor, der hat 1000 Privatrechner unter seiner Kontrolle. (was nicht wirklich viel ist… die größten Botnetze ha(tt)ben ein paar Millionen). Da ginge sich locker ein Mittelklasse-PKW nur mit dem Verkauf der Kontodaten aus.

Wie kommt das Zeug auf meinen Rechner?

Das sind die dre Hauptkandidaten für Malwarebefall (meiner Meinung nach…)



Antispyware will eingeschaltet sein



Internet Explorer ist wachsam

Das sind oft die „Bösen“ PlugIns im Browser—wenn man sie nicht aktuell hält

Meist sind Betroffene ratlos, wenn es darum geht, herauszufinden, wie sie ihren PC überhaupt mit Schadsoftware infiziert haben konnten. Früher kannte ein Schädling nur einen oder zwei Verbreitungswege. Vorbei… heute gibt‘s zig Möglichkeiten.

Die häufigste heutzutage sind Webseiten. Haben die E-Mail als Verbreitungsweg schon längst abgelöst.

Grundsätzlich: Keine Schadsoftware kann einen Webbrowser angreifen. Angriffe erfolgen immer über den Inhalt der Webseite selbst. Die häufigsten Einfallstore für mw sind demnach Java, Adobe-Reader und Flash. Es nützt demnach auch nichts, schön brav Windows7 mit Updates aktuell zu halten, wenn die Plugins des Browsers es nicht sind.

Das ist jetzt nicht unbedingt die Schuld von Microsoft. Was können die dafür, dass Adobe überproportional oft sicherheitsbedenkliche Software ausliefert. Windows7 ist nur eine wundervolle Plattform darunter, um dem Schädling ein zu Hause zu bieten.

Die Crux ist ja, dass es mit den indoktrinierten Updates von Windows und dem obligatorischen Virenscanner heutzutage nicht getan ist. Darum auch immer die Standardfrage nach einem Virenbefall: *„wieso, i hob doch e ollas aktuell“*. Abgesehen davon, dass das meist auch nicht stimmt, wenn man auf alles raufklickt was nicht bei drei auf den Bäumen ist.

Die Updateaufforderungen der Plugins werden oftmals gnadenlos weggeklickt. Es funktioniert ja auch so. Dass die Updates aber mitunter auch Sicherheitslücken stopfen…vergiss es.

Somit ist der Normaluser immer mit einer mehr oder weniger lästigen Updateorgie konfrontiert.

Windows-Office-Skype-Messenger-ICQ-Flash-Adobe_Reader- Quicktime-Realplayer-iTunes-Silverlight-Java-Virenscanner-Adaware-Spybot-CCleaner-Tuneuputilities, Defender… *bist depat?*

Ja, es ist meist mit einem Mausklick getan, und der Normalanwender hat dann sogleich drei Virenscanner und vier Bars im Webbrowser automatisch dazu installiert, weil er bei den Updates ein „Hakerl“ wo wegzuklicken vergisst.

Das klappt auf lange Sicht nicht. Ich kenne genug User mit einem aktuellen Windows7, aber der Flashplayer ist schon gut eineinhalb Jahre alt. Das wird auf Dauer auch nicht gut gehen.

Das Problem sind die verschiedenen Quellen der Software, die die Wartung so „unfreundlich“ machen.

Einer meiner Gründe für Linux. Sämtliche Software kommt von einer Quelle > dem Repository (der Quelle) meines Linux. Ob Flash, Skype, Instant-Messenger, PDF-reader oder Webbrowser.

Alles wird mit den automatischen Updates aktuell gehalten. Darum kommen da auch nicht periodisch so Pop-Ups mit Updateaufforderungen wie bei Windows. (Java…das nervt)

Die Updates laufen im Hintergrund…ohne Prozentanzeige beim Herunterfahren (das nervt auch bei einem Windowsupdate…). Und beim anschließenden Neustart erst…

Was hab ich schon geflucht, wenn der Außendienstler vor Ungeduld die Kiste einfach abgedreht hat, weil er *„schnell weg musste“*. (beim Updateeinspielen mit der Prozentanzeige)

Nachher war‘s eh egal, weil sich Windows *„aufgehängt hatte“*, und sein Arbeitstag beendet war .

Darum halte ich Linux auch für wartungsärmer. Installieren, einrichten…fertig.

Und das System ist immer aktuell (noch einmal, auch sämtliche Software auf dem System…).

Windows7 ist ja nicht schlecht. Aber eins kannst Du Dir sicher sein. Sobald was nicht klappt, ist meist Schadsoftware im Spiel. *„net scho wida neich instaliern, bitte net“*. Selbst mit deinem sechs Monate alten Image sitzt auch ein Zeitl vor der Kiste, um dann genervt festzustellen *„scheisse, meine mäls hob i net gsichert“.*

Wenn bei Linux was nicht klappt, ist es meist abgedreht oder der User hat das Administratorkennwort und *„hat einmal das System erkundet“. Klonk.*

I hob jo nix wichtiges drauf…

Viele Anwender wähnen sich noch immer vor Schadsoftware sicher, weil auf ihrem PC ja keine so wichtigen Daten lägen und sich Hacker nicht mit einfachen Privatrechnern zufrieden geben. Das ist grundsätzlich falsch.

Privatanwender sind nach wie vor das Hauptziel von Schadsoftware.

Diese hat neben dem Auslesen verschiedenster Daten auch das Ziel, möglichst viele - und zwar ausdrücklich – Privat-PC zu Bots zusammen zu schließen. Allein die Menge der ausgespähten Daten ist schon mal ein Hammer in Bezug auf die Gewinnmaximierung (siehe Preistabelle oben)

Bots

Was ist ein Bot? Software, die automatische Aufgaben über das Internet ausführt. Darunter kannst Du Dir jetzt alles vorstellen. Ferngesteuerte PC, Angriffe auf Firmen, Erpressungsversuche, Lahmlegen von Webservern, Spamverteiler einrichten, Datenverkehr verschleiern, noch mehr Malware verbreiten, illegale Daten hosten, andere Bots aufbauen und mit Konfigurationsfiles versorgen…

Ist alles illegal und bringt fette Kohle. Selbst wenn zwischendurch ein paar Tausend Rechner gesäubert (neu installiert) werden…die monatliche Infektionszahl liegt im fünfstelligen Bereich. 30.000 Webseiten werden mit schädlichem Code präpariert. Täglich. Die schiere Menge macht‘s.

Es ist auf alle Fälle lukrativer, 1000 Privat-PCs zu übernehmen, als einen Webserver einer Firma.

Wenn einer von den Privat-PCs neu installiert, sind immer noch 999 Maschinen unter fremder Kontrolle. Den Firmenserver „verliert“ er bei einer Neuinstallation aber vollständig.

Immer vorausgesetzt, dass die Schadsoftware überhaupt entdeckt wird. In Firmenumgebungen dank der dortigen Ressourcen an Mensch und Technologie wahrscheinlicher. Im Privatbereich starrt man gebannt auf die Ergebnisliste von „McAffee-Stinger“…na dann viel Glück.

Was aber tun, wenn der geliebte Virenscanner anschlägt? Quarantäne, löschen, Datei umbenennen, Reparaturversuch…?

Kommt die Meldung während eines Downloads, gibt es Hoffnung, dass der PC noch nicht in Gefahr ist. (falls die Datei noch nicht ausgeführt/angeklickt/geöffnet wurde)

Hier könnte das Löschen der Datei reichen.

Falls die Datei aber schon einmal geöffnet wurde in der Vergangenheit, musst Du davon ausgehen, dass der Schädling schon aktiv war. (oder noch immer ist). > Neuinstallation und gesicherte Dokumente auf Malware prüfen. Sorry…da führt kein Weg vorbei. Außer Du hast ein sauberes Image.

„und, wos wors fir a Virus?“, fragen mich die Leute immer, wenn ich ihre Box neu installiert habe. *„Keine Ahnung“*, entgegne ich immer. Erstens weiß ich's wirklich nicht, und selbst wenn ich es wüsste, was bringt es?

Das System war nicht aktuell… oder der User hat wo raufgeklickt. Es ist immer eines von den zwei Dingen, die dafür verantwortlich sind. Immer.

Was mach’ ich bei Schädlingsbefall?

- Rechner ausschalten. Am besten Ausschaltknopf drücken, sodass das System auch nichts mehr auf die Platte schreiben kann.
- Nicht in Panik verfallen
- Keine Removaltools verwenden
- Den Rechner nicht weiter verwenden
- Netzwerkverbindung physisch trennen (Kabel ziehen)
- Booten von einem Rettungssystem (Linux-Live-Cd).oben ist e ein passender Link zur Erzeugung einer Linux-Live-CD.
- Persönliche Daten sichern
- Festplatte und MBR löschen
- Betriebssystem installieren, konfigurieren und Updates einspielen, Autorun-Funktion deaktivieren (Standard bei Windows7.kontrollieren!)
- Gesicherte Daten auf Schädlingsbefall prüfen und dann einspielen
- Sämtliche Passwörter am System tauschen
- Sämtliche angeschlossenen Datenträger (USB-Sticks, externe Festplatten.)formatieren
- Kontoauszüge in den folgenden Monaten sorgfältig prüfen
- eine Backupstrategie überlegen (worst case Szenario)
- Eigenes Verhalten hinterfragen.

„Illegale Schnäppchen“ in den Grauzonen des Internets und dem „Hacker-Underground“ sind nach wie vor extrem beliebt. Bei den Hackern und den Endanwendern gleichermaßen. Erstere tarnen ihre Schadsoftware mitunter hinter Keygeneratoren und „Gratis-Windows7-DVDs“.

Zweitere springen bereitwillig auf den Gratiszug in Tauschbörsen auf. *„I hob no nie wos ghobt“*, tönt es dann fast entrüstet entgegen. Wie willst das überhaupt wissen. Solange alles „rennt“, lacht man überlegen die *„Trotteln aus, die sich legal Software kaufen“*.

Der entscheidende Vorteil bei legal gekaufter Software ist aber immer der: Ich habe eine vertrauenswürdige Quelle. Bei illegal gesaugter Software weiß ich nie, was drin ist. Ganz einfach. Ich brauch nicht mehr Fehlerquellen, als nötig.

Zahl einmal, installier und gut is. Kein normaler User ist daran interessiert, periodisch in der Registry sich wichtig zu machen und wpa-files einzuspielen.

Merke: Egal, welche illegal gesaugte Software du auch verwendest. Diese hat immer den Nachteil eines erhöhten Wartungsaufwandes (keine automatischen Updates…latente „Gefahr“ der Deaktivierung des Keys, negative Beeinträchtigung des Systems…)

Bringt auf lange Sicht nur Kopfweh…

Es ist auch blinder Aktionismus, dieses oder jenes „Schutzprogramm“ zu installieren, weil es gerade in einer Zeitschrift oder auf einer Webseite empfohlen wird (gerne auch jahrelang derselbe „Testsieger“).

Oder Programme die 300 Fehler in der Freeversion entdecken und sogleich wieder „gerichtet“ haben. In der zahlbaren Vollversion finden sie die restlichen 1000 Fehler. Toll, dass es so was gibt. Das kannst Du dem Otto Normalverbraucher auch schwer ausreden, weil *„wieso soi ma der wos schlechtes fakaufn…der hot jo de Föla gfundn…“*. Vergiss das. Ich frage mich auch oft, wie der ganze Müll auf die Kisten kommt, wenn ich bei Verwandten vorbeischau und sie ihr oft strapaziertes *„…konst ma schaun, ob i an Virus hob…nur schaun, damit i ma sicha bin…“* mit einer Tasse Kaffee erwartungsvoll an mich herantragen. Oder *„…is der guad der xxx-Virenscanner…?“*.

Ehrlicherweise müsste ich mit einem **„…keine Ahnung…“** antworten. Aber dann bekomm ich ja wieder schwer einen Kaffee.

Wer obige Fragen eindeutig beantworten kann, gratuliere. Ich kann‘s (wills) nicht. Wäre unseriös.

Und falls ich mal wirklich einen Schädling aufspür‘ und mit dem „herumkämpf“…wird mit einem *„…loss eam, is wurscht, des gät scho…“* der digitale Alptraum eingeläutet. Neuinstallation. Irgendwann, wenn *„ma Zeit hobn…“*.

Meist scann‘ ich das System mit dem heruntergeladenen *Sysinternals Process Explorer* und *Autoruns* (einfach googeln) und schmeiß‘ die offensichtlichen Sachen vom System (bars… zusätzliche „Schutzprogramme“, Antimalwareirgendwas, zusätzliche Virenscanner und wenn ich Zeit hab, die OEM-Ware…).

In 3 Wochen schaut‘s eh wieder anders aus. Ist nur reine Kosmetik, aber der Mensch freut sich.

Speziell „Enkerln“ haben die unliebsame Angewohnheit, den PC von Opa mit Schutzprogrammen vollzustopfen. Und gleich den gecrackten Photoshop hinterher zu installieren. Zocken am PC hat nichts mit Internetkompetenz zu tun. Der arme Opa…

Drive-by-Download

Hier gibt es nicht viel zu sagen. Warum? Weil die Infektionswege so mannigfaltig und hochkomplex sind, dass ich gar nicht weiß, wo ich anfangen soll.

Machen wir‘s kurz: Es ist unmöglich, vor Besuch einer Webseite zu bestimmen, ob sie sicher oder unsicher ist.

Das Fatale daran: Es genügt oft schon nur der Besuch der Webseite um sich zu infizieren. Ohne dass man wo raufgeklickt hat.

Das Überfahren eines Werbebanners mit der Maus kann zur Infektion schon reichen.

Seriöse Webseiten werden natürlich eher als Malwareschleuder bevorzugt, da der User so weniger Verdacht schöpft.

„SiteAdvisor“, „Webschutz“ oder *„Link-Checker“*. Diese Komponenten der Virenscanner bieten keinen ausreichenden Schutz.

Daher gibt es keine sicheren Webseiten, die man bedenkenlos ansurfen kann. Es ist ja gerade das Merkmal einer *Drive-by-Infektion*, ohne Interaktion mit dem Besucher auf dessen Rechner Malware zu installieren, wenn dieser die Seite lediglich aufruft/besucht.

Drive-by-Infektionen gelingen aber nur, wenn der Browser oder seine PlugIns Sicherheitslücken aufweisen.

Häufig ist sich das Opfer auch nicht bewusst, dass der Internet Explorer aktuell gehalten werden muss, da er von Windows für diverse Aufgaben herangezogen wird, auch wenn ein anderer Browser zum Surfen verwendet wird.

Besonders ICQ und Skype nutzen Komponenten des IE. Liegt dieser in einer veralteten Version vor, sind auch diese Chat-Dienste angreifbar - unabhängig vom tatsächlichen Chatprogramm, das diese Protokolle nutzt.

Webdesigner machen das Ganze aber auch nicht leichter.

Die Aufgabe eines Webdesigners ist es nicht, dem Leser Nützliches zu bieten. Die Aufgabe eines Webdesigners ist es, zu zeigen, wie toll er webdesignen kann. Diese Meinung könnte man beim Besuchen der meisten Websites bekommen.

Deshalb verweise ich auch immer auf eine meiner Lieblingswebseiten > **www.slackware.com**

Das Problem bei dieser Seite…man muss lesen können. (Okay, ist in Englisch). Aber mir geht‘s eher um die Aufmachung. Kein Flash oder Java Gedröhn, keine Schneeflocken oder animierte wasauchimmer… einfach nur Information. Sorry, das musste sein.

Öffentliche Wahrnehmung

Ein komplett anders geartetes Problem, auf das der Einzelne kaum Einfluss ausüben kann, ist die öffentliche Wahrnehmung bezüglich Cyberkriminalität in den Medien.

TV-Serien wie CSI oder Navy CIS, Kinofilme wie *„Password Swordfish“, „Hackers“, „Matrix“, „Das Netz“* oder *„Independence Day“* sind der Nährboden für den interessierten Endanwender.

Genauso wie die zellulitisfreien, notgeilen und immer alleinstehenden Krankenschwestern mit ihrem abbezahlten 200 Quadratmeter-Penthouse in den Vorabendserien mit der Wirklichkeit so viel zu tun haben, wie steirische Bergziegen mit Algebra.

Immer wieder erheiternd, dass Hacker auch im 21. Jahrhundert noch wie wild auf der Tastatur herumklimpern, obwohl es längst die Computer-Maus gibt.

Wenn es hier nur um Eingabe eines Codes oder einer Befehlsfolge ginge - okay, aber meist tippseln die Hacker ja ewig herum. Verschreiben die sich so oft?

Erinnert mich immer an Filme aus den 60ern, wo die Autofahrer abwechselnd 10 cm nach links und rechts mit dem Lenkrad gerudert sind, wenn im Hintergrund die Leinwand vorbeigezogen wurde :-))

Dazu noch wild aufpoppende Fenster mit Dateilisten, Videos und Binärcodes am besten wild durchmischt und auch garantiert ruckelfrei. Zum Drüberstreuen noch eine riesige Weltkarte *(aaahhh…ooooh, i äm impräst)*, am besten mit einem wachsenden Netzwerk aus Linien…wau. Viel, bunt, fehlerfrei und immer cool.

Der Filmheld steht dann hinter dem (meist adipösen, sozial ausgegrenzten, glatzerten Brillenträger …der den Häka spielen darf) flechtet noch die Fachbegriffe wie *Firewall, Hacker, Rückverfolgung, Code, Virus* und *verschlüsselt* ein und blickt dann wissend auf den Monitor…bis halt der Regisseur *„cut“* schreit.

Spitze auch, wenn man den Ermittlern über die Schulter schaut, wenn sie Datenbanken nach Fingerabdrücken oder Autokennzeichen durchsuchen. Toll animierte Benutzeroberflächen, gepaart mit schicken Einblend-Effekten (alles so schnell) und dann das ersehnte groß blinkende *„Match found“*. Die Festplatte wird mal schnell in 2 Minuten auf einen USB-Stick kopiert und eine landesweite Datenbank spuckt in spätestens 20 Sekunden ein Ergebnis aus. Wie im wirklichen Leben. Und es werden immer Firmenserver geknackt. Nie Heimanwenderrechner… vergiss‘ das.

Webbrowser

Egal, was Du nimmst. Halte es aktuell. Ob Firefox IE oder Chrome. Installiere keine Beta-Versionen, Tuningtools, Spurenverwischer, Toolbars oder Anonymizer. Das tut keinem Webbrowser gut.

Man ist nie selbst schuld, wenn der Browser abstürzt. Bedenke, mit der oben erwähnten Software kann man jeden Browser ganz schön aus dem Gleichgewicht bringen.

Natürlich ist dann immer der Browser Schuld - nie und nimmer man selbst.

Heutzutage fangen sich die Leute mit Firefox genauso viel Malware ein wie die Nutzer des Internet Explorers.

Ditto bei Chrome und Opera. Der Malware ist es egal, ob das veraltete Browserplugin auf Firefox oder dem Internetexplorer läuft. Anfällig für *Drive-By-Infektionen* ist es. Das genügt.

Und da man ja alle Funktionen der Webseite „braucht“, wird eben jedes Plugin installiert, was da des Weges kommt.

Darum halte auch und vor allem die Plugins aktuell…in Deinem eigenen Interesse.

Virenscanner

Es gibt eine Menge Leute, die von ihrem Lieblingsvirenscanner dermaßen überzeugt sind, dass sie noch immer und angesichts fortdauernder Infektionen trotz installierter Schutzprogramme weiterhin widersprechen, wenn man sie mit der Realität konfrontiert.

„Früher oder später erkennt jeder Virenscanner Malware…“. Das stimmt uneingeschränkt. Das Problem ist immer das *„später“*. Dann ist es meist zu spät…

Du kannst Hunderte Tests im Internet durchackern. Schlauer wirst Du davon aber nicht, weil es keine einheitlichen Testkriterien gibt.

Falls Du Dir bei einer Datei unsicher bist, lass' sie auf der Seite www.virustotal.com gegenchecken. Ist selbsterklärend…

Fazit: Durch den permanenten Updateaufwand sehe ich beim Heimuser weiterhin eine latente Schadsoftwaregefahr. Trotz Windows7. Daher werden Neuinstallationen auch weiterhin tägliches Brot von EDV-Supportern bleiben.

Die leidige Sache mit der vorinstallierten OEM-Bloatware will ich jetzt gar nicht andenken. Erst kürzlich wieder mal gute 20 Minuten gebraucht, um so ein Ding vollständig vom System zu bekommen. Eines!

Das Thema Malware ist auch nicht wirklich bei vielen Usern angekommen. Wird es meines Erachtens auch nie. Genauso wie Backups. Vergiss das.

Wer hat Schuld? Alle. Die User, die Softwareentwickler und die „Bösen".

Allein durch soziale Netzwerke (facebook, twitter…) wird so viel Müll so rasant in Umlauf gebracht…die schiere Menge macht's.

Heuer hab ich sicher schon 10 Privatkisten mit Windows7 neu aufgesetzt. Weniger wird's nicht werden.

Alternativen? Verwende Linux. In 10 Jahren hatte ich noch nie ein Schadsoftwareproblem, oder einer meiner Linux-Kunden. Begünstigend kommt hinzu, dass ich unter Linux nie das Administratorkennwort (root) hergebe. Das hilft auch ungemein.

Oder probier' mal Apple. Ja ich weiß…

Kenne sogar Windows-User, die nehmen fürs Surfen ein iPad und machen ihren Bürokram dann in Windows.

Ich misch' mich da nicht ein. Jeder, wie er mag. Leider wird das Thema Schadsoftware in Zukunft auch vermehrt die Smartphones betreffen. Das steht fest. Warum? Weil's die größte und unerfahrenste Zielgruppe ist. Die Heimuser.

So, wie immer gilt. Ist alles nur meine Meinung zum Thema. Könnte noch seitenlang weiterschreiben, aber eigentlich will i nimmer. Is Mitte März und wir haben 20 Grad. Was mach i noch da? Muss jetzt Radfahren gehen…

Gruß Günter

Zu den Themen Wiederherstellungspunkt, RescueCD, Systemabbild, Backup, Reparaturdatenträger, GParted:

Im Falle eines Falles
Franz Fiala, PCNEWS 123, Seite 26
http://pcnews.at/d/_pdf/n1230026.pdf

Täter „Elko"

Georg Tsamis

Kürzlich hat mein (alter) Acer AL1912 LCD Monitor den Geist aufgegeben.

Mit 1280x1024 ist er nicht mehr berühmt, gehört aber noch lange nicht zum alten Eisen.

Anfangs ließ sich durch mehrmaliges Ein- und Ausschalten das Ding wieder zum Leben erwecken, es leuchtete dann die Betriebs-LED auf, und das Bild kam auch wieder. Später kam gar nichts mehr.

Ich war verhärmt, weil ich ihn zum Arbeiten brauchte. Da vor zwei Jahren oder so ein Bürokollege (HW-Entwickler und daher gut ausgerüstet) mein altes Motherboard durch Ersetzen von zwei Elektrolytkondensatoren (Elkos) wieder zum Laufen brachte und ich doch recht glücklich war darüber, dachte ich hier auch an diese Fehlerquelle.

Elkos sind DIE "Sollbruchstelle" der Funktion elektronischer Geräte der heutigen Zeit. 5-7 Jahre und irgendeiner ist sicher (bald) kaputt.

Ich habe also - anfangs mühsam, dann mit einer Zerlegeanleitung aus dem Internet - die entstehen vermutlich dann, wenn die Elkos zu sterben beginnen :-) - den Monitor zerlegt, das Power Supply Board ausgebaut und die Komponenten genau unter die Lupe genommen.

Tatsächlich: Zwei Elkos hatten schon statt eines schön flachen "Daches" ein leicht bombiertes: ein sicheres Zeichen nahen oder schon eingetretenen Todes:

Technotronic hat mir die Ersatz-Elkos mit gleichen Daten um je EUR 1,00 verkauft.

Ausgelötet, eingelötet, zusammgesteckt, ausprobiert: GEHT WIEDER !!!!

HURRA, war das eine Freude!

Fertig zusammengebaut tut er jetzt wieder seinen Dienst als ob nix geschehen wäre. Um EUR 2,00.

Ein Power Supply Board als Ersatz ist käuflich nicht erwerbbar. Reparieren könnte man es lassen (allein diese Auskunft bei einer 0900-Nummer hat mehr gekostet als die Elkos).

Die moderne Wegwerfgesellschaft kennt kaum mehr derartige Reparaturen. Vielleicht hätte ein kleiner Fernsehgeräte-Laden, der noch selber repariert und nicht nur einschickt, die Sache auch gemacht. Aber ich wäre vor der Frage gestanden, ob sich das Geld noch auszahlt, das ich in die Reparatur stecken müsste. Denn neue Monitore sind ja auch nicht gar so teuer wie Arbeitszeit von sagen wir 1,5 Stunden schnell werden kann. Gerade, wenn er das Gerät nicht schon kennt. Die Gefahr wäre groß gewesen, dass das Ding wegen zwei defekten Elkos als Elektronikschrott den Weg zum mühsamen und teuren Recycling antreten hätte müssen.

Der Lötkolben, mit dem ich die Arbeit gemacht habe, ist danach in den Elektroschrott gewandert: er war schon ca. 40 Jahre alt und die äußere Isolierung des Netzkabels war bereits hart und nur mehr in Bruchstücken vorhanden. Ich hab mich fast gefürchtet beim Löten und war SEHR vorsichtig.

Einen neuen Lötkolben und einen Lötsauger hab ich mir einfach schon deshalb geleistet, weil ich mir so viel Geld erspart hatte und recht glücklich war.

Hier noch ein Link zum Lesen (weiterführende Info)

http://www.lcd-repair-review.com/bulging-capacitor