E-rules
Umgang mit dem Internet

Klaus Daubes umgang mit dem Internet

Alle wochen bald lesen oder hören wir neue horror-meldungen über viren, trojanische pferede, würmer und anderes getier, das uns das leben mit dem Internet vermiest.

Was kann ich nebst der abstinenz von gefährlichen inhalten tun, damit mir diese an Hyronimus Bosch erinnernden szenen möglichst wenig anhaben?

Diese zusammenstellung von verhaltens-regeln ist meine ganz persönliche ansicht. Leute mit viel mut und genügend zeit zum kurieren von seuchen werden ganz andere vorschläge machen.

Klaus Daubes verhaltens-regeln

Die hier zusammen gestellten regeln fussen auf meiner eigenen erfahrung und stellen nicht immer das allgemein übliche dar. Schon gar nicht sind diese regeln im sinne des software-giganten Microsoft. Es ist dem einzelen nicht immer leicht, diese regeln umzusetzen, da etliche einstell-möglichkeiten von programmen kompliziert und unverständlich sind.

Diese regeln schützen nur 'gegen aussen'. Wer selbst im trüben fischt, bekommt natürlich auch gruselzeugs an die angel…

Distanziere Dich von der meute

Seit uralten zeiten lacht das jagdglück eher, wenn nicht nach einzelgängern gesucht, sondern einer meute abgepasst wird. Moderne pirscher (hacker, abzocker, schurken und software piraten) halten es da nicht anders.

Deshalb ist es gut, sich von der meute abzusetzen und nicht alles zu tun, um 'überall' dabei zu sein:

- Wer die software eines unersättlichen SW-giganten einsetzt, braucht sich nicht zu wundern, dass er zielscheibe von attaken aller art wird. MS bietet einem viren-verbreiter das grösstmögliche arbeitsfeld!
- Wer sich in allen möglichen news-groups und chat-rooms tummelt, ist bald als opfer enttarnt, da viel online (siehe *Schnelle leitung, schnelle infektion* auf seite 4).

Ein virus ist ein programm

Viren können heute nicht nur als gewöhnliches programm auftauchen, sondern auch als macros in dateien, die von einem programm (text-verarbeitung, spread-sheet) dann ausgeführt werden. Sehr gefährlich sind Visual Basic programme (.vbs)!

Normale bilder (mit den endungen .gif, .jpg etc.) sind statisch. Programmbezogene dateien für zb. PhotoShop können sogenannte history-daten enthalten, das ist eine liste von zuletzt ausgeführten aktionen - und hier öffnet sich ein tor für vollkommen neuartige viren.

E-mail ist statisch, aber …

Ebenso statisch ist die reine e-mail meldung. Es gibt nun aber leute, die mit ihrem e-mail programm HTML erzeugen und verbreiten, und hier könnte ein Java applet oder ein JavaScript drin sein. An sich laufen Java applets in einer sand-box, in einem sicheren bereich innerhalb eines rechners, aber sicherheitslöcher gibts da immer.

Das übelste sind aber die von MS in die welt gesetzten *Active-X-Controls* (OCX)[1)], die tatsächlich aufs betriebssystem zugreifen können, und damit sehr gefährlich sind.

Daher sollte ein e-mail programm nur gewöhnlichen text erzeugen und darstellen. Bessere darstellungen sollten als anhänge verschickt werden (und nicht eingebunden!!). Das entspricht nicht den standard-einstellungen von MS-software.

Anhänge **nie** mit doppel-klick öffnen!

Attachements (anhänge) sollen nie mit doppelklick geöffnet werden (siehe *Banne den doppelklick* auf seite 4), sondern mit dem kontext-abhängigen menü (rechte maustaste) in einen sicheren download-bereich gespeichert werden (siehe *Download immer in drei schritten* auf seite 3).

Automaten sagen nicht, was sie gerade tun

Wer zu faul ist, einzelne schritte (zb beim herunter laden von daten oder programmen) immer wieder manuell auszulösen, muss sich nicht wundern, wenn hinter seinem rücken unliebsame dinge passieren:

- Wenn der browser einfach alles, was er kennt, direkt öffnet, können macro-viren nur so ausschwärmen.
- Wer einem heruntergeladenen programm erlaubt, sich selbst zu entpacken und grad auch noch zu installieren, kauft sich doch den sensenmann im sack!

Download immer in drei schritten

Aus diesen gründen soll ein download grundsätzlich in zwei bis drei schritten ausgeführt werden. Das gilt auch für e-mail anhänge (attachements):

1 Den browser so einstellen, dass er nur HTML, bilder, sound und video darstellt. Word, Excel und andere programme sollen nicht automatisch gestartet werden! OCX sollen nicht akzeptiert werden. Java ist relativ sicher, JavaScript *ist* sicher.

   Für den download ein eigenes verzeichnis verwenden: `I:\temp\download\`.

2 Nach dem download einen virenscanner über dieses verzeichnis laufen lassen. Neuere spezies können auch in komprimierte daten schnüffeln. Nur das neueste ist hier gut genug. Immer wieder aktualisieren ist wichtig!

3 Von Word- und Excel dateien interessiert meist nur der inhalt, nicht die enthaltenen macros und tollen darstellugen. Daher ist es am sichersten, solche dateien mit einem speziellen anzeige-programm anzusehen und/oder zu drucken[2)], statt sie wirklich zu öffnen (was ja nur für änderungen nötig wäre).

4 Erst jetzt ein programm aus der temporären verzeichnis heraus installieren.

---

1 *internet world* oktober '99, s. 12 (http://www.internetworld.de)

2 Ich habe auf meinem system das programm *QickView Plus* installiert, mit dem über 200 verschiedene datenformate angesehen werden können - selbst exotische datenbanken.

Scherzkekse

Etliche leute haben grosse angst vor den sogenannten cookies (kekse). Dies sind daten-schnipsel, die vom browser in einer datei abgelegt und wieder gelesen werden können. Sie sind zb notwendig für den 'elektronischen einkaufskorb', da im web alle seiten vollkommen unabhängig voneinander sind und sonst der kunden-bezug einer bestellung verloren geht.

Mit cookies können keine daten aus-spioniert werden. Hingegen kann ein cleverer e-commercer (eine bestimmte anbieter-firma), bei dem man häufig vorbeikommt das kunden-verhalten studieren (was bevorzugt er?). Aber das kann jeder kaufmann um die ecke auch, wenn er nicht schläft.

Sinnvoll kann es sein, den browser so einzustellen, dass er cookies nicht über die surf-session hinaus aufbewahrt.

Banne den doppelklick

Mit doppelklick wird eine datei geöffnet - und das geschieht im allgmeinen mit dem zugeordneten programm. Ist immer klar, welches programm einem e-mail anhang zugeordnet ist?

Wenn es sich um ein Word- oder Excel-dokument handelt, kann dieses macros enthalten, die beim öffnen des dokuments ablaufen, noch bevor der benutzer etwas sieht!

Es gilt hier das unter *Download immer in drei schritten* auf seite 3 gesagte.

Gratisangebote haben ihren preis

Viele surfer verwenden heute den gratis-zugang zum Internet, den ihnen der telephon-provider anbietet. Dies kann folgende auswirkungen haben:

- Weil der service überrannt wird, haperts mit der stabilität und sicherheit des zugangs.
- Da solche dienste mehrheitlich von 'unbedarften' benutzern' (zb nicht von firmen) in anspruch genommen werden, sind sie ein ideales tummelfeld für tunichtgute.

Schnelle leitung, schnelle infektion

Es ist nicht nur für den surfer interessant, schnell durchs netz zu sausen - auch den finsteren gesellen kommt das sehr zupass[3)]. Im gegensatz zu modem-verbindungen sind nämlich die DSL- und kabel-modem-verbindungen immer aktiv, wenn der PC eingeschaltet ist. Damit werden fleissige leute am leichtesten das opfer von attacken... Zudem kann der so okkupierte PC auch für attacken auf andere netz-teilnehmer missbraucht werden. Aus dem opfer wird so grad auch noch ein täter.

3 Internet World 2000-04, p 12: *Sicherheitsrisiko High-speed zugänge*.

Eine verbindung aufbauen und sie nach gebrauch wieder schliessen, ist eine sehr gute sicherheits-strategie. So erhält man auch jedesmal eine andere IP-adresse (numerische netz-adresse), die in keinem verzeichnis aufbewahrt wird.

Keine verbindung ohne überwachung

Der ganze verbindungs-zauber muss so aufgebaut sein, dass eine bestehende verbindung mit dem Dial-Up Monitor (DUM) angezeigt wird. Leider bieten die diversen Windows hier die absolute verwirrung für den laien.

Ausserdem gibts programme (zb UBS Telebanking), die kalten a… wählen, mit abgestelltem modem-lautsprecher und unter umgehehung des normalen einwähl-prozederes, das den DUM aktiviert! Für solche programme unbedingt den DUM vorher aktivieren!

Wichtige dinge gehören unter verschluss

Verschlüsselungen machen nur dann sinn, wenn sie nicht für *alles mögliche*, sondern nur für *alles nötige* eingesetzt werden. Denn safes, tresore, dicke schlüsselbunde und verschlüsselte e-mail wecken den verdacht, dass da 'was zu holen ist!

Viele leute haben angst vor der übertragung der kreditkarten-nummer über's netz. Wenn mit einer 'sicheren übertragung' gearbeitet wird (der browser zeigt dann 2-3 schlüssel oder schlösschen), ist das kein problem[4]. Wichtig ist aber, solche daten nur mit vertrauen-erweckenden firmen auszutauschen. Denn hacker hören heute nicht mehr den e-mail bzw browser-verkehr ab, sonder attackieren schwache firmen und klauen ihnen die dort abgelegten daten.

Verschlüsseln von e-mail[5] (zb mit PGP = Pretty Good Privacy) macht für privatleute kaum sinn, es sei denn, sie verbreiten kom-primittierende meldungen! Für firmen ist's da schon anders. Betriebsgeheimnisse werden auch heute noch aus-spioniert.

Viele jäger sind des hasen tod

Wer für alles und jedes neue passwörter einsetzt, kann sie doch nicht im kopf behalten und schreibt sie auf, womöglich noch in den computer in einer datei, das `passwords.txt` heisst. Ist da 'mal 'wer drin, sind weitere türen leicht zu öffnen.

Ich halte viel mehr von einem möglichst langen, universellen passwort, das nichts mit meinem leben zu tun hat - also keine geburtstage, namen usw. Besser sind zahlen-folgen *aus* irgend einer mathematischen konstante, zb e (2.718281828459045…) oder goldener schnitt (1.618033988749848…). Aber bitte nicht den anfang von pi, das kennt jeder[6]. Auch aztekische götternamen geben gute passwörter ab, können aber nicht so universell verwendet werden.

---

4 Swiss Internet User Group unter der überschrift *Kreditkarten - Do's und Dont's*.
5 TA-computer bund vom 2000-02-28 (*Sichere elektronische Post*).
6 Du nicht? 3.14158979323846 2643…

So 8 ziffern sollten die PW schon lang sein, auch wenn in etlichen anwendungen dann nur weniger davon eingesetzt werden können (Postomat verträgt zb nur 4 ziffern - das halte ich nicht gerade für einen schutz).

Büchsenfleisch en masse

Wer eine e-mail adresse sein eigen nennt, wird über kurz oder lang von irrelevanten und anderweitig unerwünschten sendungen heimgesucht - spam[7]. Dieses wort kennzeichnet sogenannte unerwünschte e-mail, die en-masse versandt wird. Spam war eine US marke für billiges dosenfleisch…

Die spammer kommen auf die verschiedensten arten zu e-mail adressen. Dreiste typen schicken einfach 'was an alle info@*domain-name*.ch. Die domain-listen können in vielen ländern ganz leicht geklaut werden (in CH nicht so leicht).

Spam abwehren

Grundsätzlich so verhalten:

- Nicht antworten, auch wenn da drin steht, man solle zwecks löschung aus der liste mit REMOVE antworten. Jede antwort bestätigkt die korrektheit der vollgemüllten adresse!
- Im browser nicht eine echten e-mail adresse angeben. Das mindeste ist eine von menschen (aber nicht programmen) durchschaubare verschleierung, zb statt `klaus@daube.ch` ➔ `klaus@ebuad-rueckwaerts.ch`.
- In chat-groups keine e-mail adresse 'fallen' lassen und in news-group mit einer verschleierten adresse arbeiten.
- Das mail-programm mit eingangs-filtern ausrüsten, dass zb mails mit 'big money', 'nice girls' und anderem gleich in den papierkorb wandern. Jedes anständige mail-programm erlaubt das definieren solcher filter - ist aber mit arbeit verbunden.

Divide et impera

'Teile und herrsche' war der wahlspruch von Ludwig dem XI, um aus der spaltung der gegner gewinn zu ziehen. Dieses prinzip wird auch in der modularen programmierung angewendet, um aufgaben klar abzugrenzen und damit fehlerquellen voneinander zu isolieren.

Die von MS praktizierte "enge integration" von browser und betriebssystem (bei IE 4 und insbesondere IE 5) ist das pure gegenteil dieses prinzips. Nebst der unübersichtlichkeit einer eierlegenden wollmilchsau ist dieses gebilde auch sehr gefährlich:

Wenn das datei-system praktisch identisch ist mit dem browser, kann nicht mehr unterschieden werden, ob ein befehl (zb lösche datei xyz) von der tastatur, einem anderen programm oder aus dem netz kommt…[8] Wer den briefträger immer bis in die woh-

7 http://www.siug.ch/positionen/SIUG-Spam.shtml

nung kommen lässt, wird bald auch ungebetene gäste auf der matte haben.

Daher: keinen "aktive desktop" in Windows etablieren und auch in W2000 oder XP den browser als eigenständiges programm installieren und nicht zur dateiverwaltung einsetzen.

Standard-einstellungen sind nur für ganz dumme

Windows und andere MS-applikationen unterstellen dem benutzer dass er nicht weiss, was er eigentlich will. Daher sind solche programme unmittelbar nach der installation recht arrogant und

- Verstecken wichtige information (datei-explorer zeigt die endungen registrierter 'datei-erweiterung' nicht an ➔ anzeige einschalten, sonst sehen sie bei e-mail attachements nicht die gefährliche endung xxx.**vbs** (wie zb der I love You virus).
- Word etc. verschlampt allen verfügbaren diskplatz mit 'schnell speichern' ➔ unbedingt abstellen. Ein e-mail attachement mit einer solchen Word-datei enthält allen möglichen inhalt inklusive ihres tagebuches.
- System-dateien mit den den attributen 'versteckt' oder 'system' werden im datei-explorer nicht gezeigt, also meint man, es gäbe sie nicht und könnten nicht von viren angegriffen werden ➔ anzeige aktivieren.
- Gefährliche funktionen wie Windows Scripting Host sind aktiv, ohne dass der benutzer das will, den viren-hackern aber sehr zu pass ist ➔ ist nicht so leicht zu de-installieren.
- und, und, und

Eine brandmauer als ultima ratio

Firmen betreiben ihre internen netze schon lange hinter einer firewall, einer brandmauer. Das sind eigene netz-rechner, welche das interne netz gegenüber dem externen (Internet) anonymisieren und abschotten. Jeder eingehende verkehr wird in diesen rechnern analysiert, ob er auf bestimmte dinge zugreifen darf oder nicht. Ebenso kann der ausgehende verkehr analysiert und ev. abgeblockt werden.

Für den gewöhnlichen surfer ist das mehr als nur mit kanonen auf spatzen geschossen - vor allem viel zu teuer. Es gibt nun aber seit einiger zeit programme[9)], welche eine solche firewall auf dem eignen PC nachbilden. Der browser oder das e-mail programm verkehren also nicht direkt mit dem Internet, sondern nur über dieses spezielle programm.

Seit ich ein solches programm (Zone Alarm) installiert habe, sehe ich, dass pro stunde surfen etwa eine attacke bei mir abprallt. So alle 14 tage ist eine deftige dabei!

8 Javaboutique.Internet.com: *New Security Vilnerbility found in Internet Explorer (IE4, IE5)*.

9 PC-Guide 3/2000 s. 128; PC-Magazine December 1, 1999, p 247.

Programm-einstellungen

Details hängen von der tatsächlichen konfiguration ab:

- Windows version, Mac OS version.
- Browser (Opera, Netscape, IE, etc)
- E-mail programm (Pegasus, Eudora, Communicator, Outlook[10] etc)

Betriebssystem

- ❒ Browser *nicht* in den desktop (dateiverwaltung) integrieren!
- ❒ Gemeinsame nutzung von disks verhindern.
- ❒ Spezielles verzeichnis für downloads einrichten.
- ❒ Viren-scanner stets à jour halten.
- ❒ Windows Scripting Host abschalten bzw. einschränken[11].

Internet-zugang

- ❒ Ankommende telephon-verbindungen nicht abnehmen.
- ❒ Verbindung automatisch abbrechen, wenn > 5min inaktiv.
- ❒ Dial-Up Monitor aktivieren.
- ❒ Nur das netzwerk-protokoll TCP/IP aktivieren.[12]
- ❒ Lieber etwas zahlen als risiken eingehen.

Browser

- ❒ Cookies am ende der session löschen.
- ❒ Identität verschleiern (zumindest die e-mail adresse).
- ❒ Direktes starten von applikationen auf ein minimum setzen. Keinesfalls macro-fähige anwendungen direkt starten lassen.
- ❒ Active-X- controls verbieten.

E-mail client

- ❒ Filter zum abfangen unerwünschter mail einrichten.
- ❒ Provider suchen, der nicht als relais eingesetzt werden kann.
- ❒ Vom provider anti-spam massnahmen bestätigen lassen.
- ❒ Meldungen als normalen text erstellen und keine HTML mail erlauben.
- ❒ Zusätzliche daten als anhänge, nicht als 'einschlüsse' senden.
- ❒ Für heikle sachen verschlüsselung vorsehen. Mit empfänger (auf anderen kanälen, zb FAX, brief) absprechen.

---

10 Als viren-sauger bekannt: internet-world, november '99, s. 82.
11 Viele viren wie zb I-LOVE-YOU arbeiten mit Visual Basic!
12 TA-Computerbund 2000-04-10: *Schlupflöcher für Vieren im DFÜ Netwerk stopfen*).