INFONEWS

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

www.goSecurity.ch
Mit Sicherheit an der richtigen Adresse.

Malware

Die Gefahren und Varianten von Malware haben in den letzten Wochen massive Ausmasse erreicht. Täglich kommen ca. 2500 neue Schädlinge dazu. Daher ist es wichtig, sich geeignet dagegen zu wappnen.

Dieser INFONEWS 2/11 geht auf folgende Fragen ein:

- Welche Arten von Malware gibt es?
- Welche Massnahmen können ergriffen werden?
- Wie verändert sich die Bedrohungslage in Zukunft?

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

1 Malware

Malware steht für Malicious Software. Sie beinhaltet ein riesiges Schadenspotential und kennt raffinierte Angriffsarten, wie beispielsweise Social Engineering, Backdoor Erstellung oder Vulnerability-Nutzung. Nach dem Bundesamt für Informationssicherheit in der Informationstechnik BSI ist Malware nach menschlichem Fehlverhalten und technischen Defekten die 3. grösste Bedrohung für Informationssysteme. Die Unwissenheit oder Nachlässigkeit von Benutzern und Administratoren sind mitverantwortlich für die grosse Verbreitung von Malware. Typische Charakteristiken von Malware sind manuelle oder automatische Aktivierung, bösartige Intelligenz, unterschiedliche Zielsysteme, diverse Trägersysteme und Transportwege.

Unter Malware wird zwischen Viren, Würmern und Trojanischen Pferden unterschieden. Die Grenze zwischen Viren, Würmern und Trojanischen Pferden ist oft fliessend. Der Hauptunterschied zwischen Viren und Würmern liegt grundsätzlich in ihrer Verbreitungsstrategie. Während Viren auf direkte Mithilfe der Systembenutzer angewiesen sind, verbreiten sich Würmer selbstständig. Die Verbreitungsgeschwindigkeit bei Würmern ist um ein Vielfaches höher als bei traditionellen Viren. Innert weniger Minuten kann sich ein Wurm weltweit verbreiten. Als Vergleich dazu brauchten traditionelle Boot-Viren x Monate, um von Kontinent zu Kontinent zu gelangen.

In den 90er Jahren waren Bootviren, wie zum Beispiel der FORM-Virus, am meisten verbreitet. Heute bilden Würmer, wie zum Beispiel der SQL Slammer, Conficker, TDL-4 und weitere den grössten Anteil der digitalen Parasiten. „The WildList Organization International“ listet monatlich die Malware auf, die im Internet verbreitet ist. Diese Liste unterscheidet sich stark von denen der Antivirenhersteller, da diese auch so genannte Laborviren berücksichtigen. Aktuelle Informationen finden Sie auch in den Security News unter http://www.gosecurity.ch/security-news/.

Die grosse Anzahl von Malware wird u.a. durch benutzerfreundliche Malware-Construction Kits erreicht, wie sie auf diversen, einschlägigen Websites heruntergeladen werden können.

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

1.1 Viren

Viren zählen nach klassischer biologischer Sichtweise nicht zu den Lebewesen, da sie keinen eigenen Stoffwechsel besitzen und sich ohne fremde Hilfe nicht fortpflanzen, bzw. vermehren können."

Ähnlich wie biologische Viren, bezwecken Computerviren, sich schnell und häufig zu vermehren. Da dies nicht ohne fremde Hilfe möglich ist, sind sie auf unachtsame Benutzer angewiesen, welche zum Beispiel viren-verseuchte Mails, Dateien oder Programme öffnen. Nach genügend langer "Fortpflanzungszeit", geben sich die meisten Computerviren zu erkennen, indem Sie zum Beispiel Mitteilungen auf dem Bildschirm anzeigen oder bösartig Daten zerstören.

1.1.1 Virentypen

Die Vielfalt von Computerviren ist gross. Dazu zählen folgende Typen:

- **Datei-Viren**
  Dateiviren infizieren ausführbare Programmdateien (z.B. .COM oder .EXE). Durch das Starten eines infizierten Programms werden sie aktiviert, erhalten die Kontrolle über das System und vermehren sich, indem sie andere Programmdateien infizieren.
- **Boot-Viren**
  Bootsektor-, MBR und Partitionsviren befinden sich auf dem Teil der Diskette/Festplatte/CD-ROM/USB-Stick, auf welchem beim Booten des Systems automatisch zugegriffen wird. Befindet sich in diesem Teil ein ausführbares Programm, so wird dieses ausgeführt. Handelt es sich bei diesem Programm um einen Virus, wird dieser ausgeführt, bzw. aktiviert.
- **Makro-Viren**
  Makroviren verbreiten sich über infizierte Datendateien, wie z.B. Microsoft Word oder Excel und sind grundsätzlich unabhängig vom eingesetzten Betriebssystem. Eine Vielzahl dieser Dateien (Word, Excel, Access usw.) beinhalten eine "Startsequenz", welche mit dem Öffnen der Datei automatisch ausgeführt wird. Die "Startsequenz" zum Beispiel von MS Word heisst AutoOpen oder unter MS Access Autoexec.
- **Hybrid-Viren**
  Ein Hybridvirus kombiniert die Eigenschaften und Fähigkeiten mehrerer Virentypen. Es existiert z.B. eine Vielzahl von Hybridviren, welche sowohl Boot- wie auch Dateiviren sind.
- **„Exoten"-Viren**
  Weniger verbreitet, dennoch teilweise gefährlich sind „Exoten"-Viren. Zu diesen zählen u.a. Help-Viren, welche HLP-Dateien infizieren, PDF-Viren, die auf Adobe Acrobat Produkten laufen oder Flashviren , welche Flash- bzw. Shockware-Plug-Ins Anweisungen des Browsers ausführen.

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

1.2 Würmer

Würmer zählen nach klassischer biologischer Sichtweise zu den Lebewesen, da sie einen eigenen Stoffwechsel besitzen und sich ohne fremde Hilfe fortpflanzen bzw. vermehren können."

Der Computerwurm vermehrt sich im Gegensatz zum Computervirus ohne fremde Hilfe. Sobald sie einmal "zum Leben erweckt" wurden, verbreiten sie sich selbständig im Internet oder in Firmennetzwerken. Dabei nutzen sie beispielsweise die E-Mailfunktionen einzelner Computer oder Schwachstellen in Systemen. Nimda, einer der bekanntesten Würmer, verwendete eine Vulnerability im Microsoft Internet Information Server (IIS 5.0) und infizierte innert kürzester Zeit Millionen von IIS-Systemen. Aber auch der SQL Slammer konnte eine Vulnerability des Microsoft SQL Servers 2000 erfolgreich ausnutzen.

1.3 Trojanisches Pferd

Kassandra warnte die Trojaner vor vielen Gefahren, einschliesslich des hölzernen Pferdes, mit dem die Griechen in die Stadt eindringen würden, aber sie wurde als Wahnsinnige abgetan.

Ein Trojanisches Pferd (oft auch irrtümlich als Trojaner bezeichnet) ist ein Programm, welches neben seinen offensichtlichen Aktionen, noch andere, verdeckte und unerwünschte Aktionen ausführt. Sie bezwecken in der Regel, Daten und Passwörter zu stehlen oder die Kontrolle des Systems an "Fremde" zu übergeben. Z.B. kann ein Trojanisches Pferd den Tastaturpuffer des Benutzers überwachen und allfällige Kennwörter, Kreditkartennummern oder Bildschirm-Schnappschüsse an Dritte senden oder den Rechner fernsteuern um damit Server anzugreifen oder Spam zu verschicken.

1.4 Scareware

In den letzten Wochen haben die Meldungen über Scareware stark zugenommen. Dabei wird versucht, dem Benutzer mit einer gefälschten Virenwarnung Angst zu machen und ihn zum Besuch einer Webseite oder zum Download einer Software zu bringen.

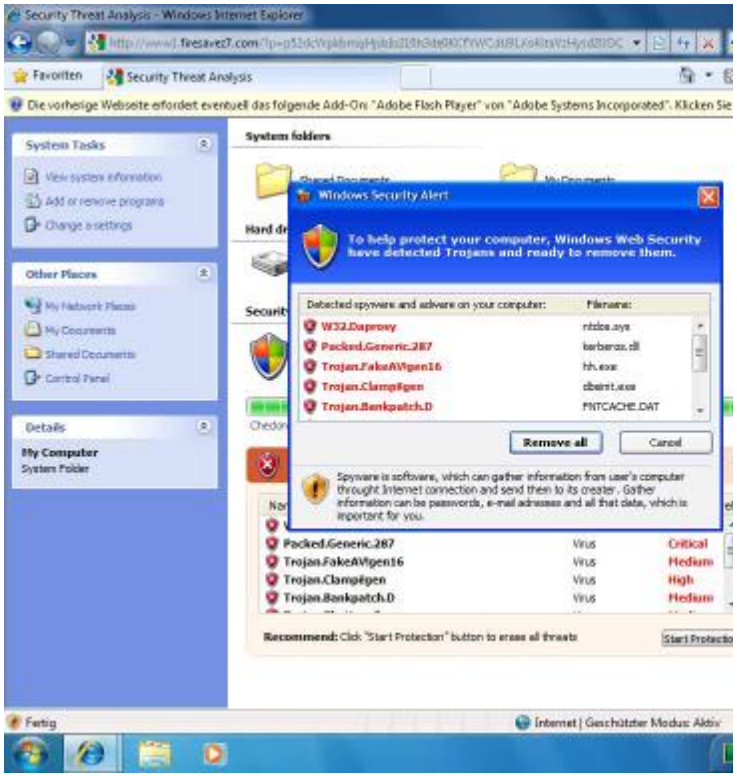
Bei der Suche nach Informationen im Internet erscheint plötzlich ein Fenster mit einer Virenwarnung (nachfolgende Seite). Das Fenster zeigt den gewohnten „Eigene Dokumente“-Ordner mit einem vorgelagerten, laufenden Virenscanner mit Virenfunden. Die erste Reaktion ist sicherlich ein grosser Schreck auf die unerwartete Meldung. Da liegt es nahe, auf den Button „Remove all“ zu klicken.

Mit dem Klick auf diesen Button wird in der Regel eine Bestellseite für ein, meist nutzloses, Antivirentool geöffnet. Bevor dieses Heruntergeladen werden kann, muss aber zuerst die eigene Adresse und natürlich die Kreditkartedaten angegeben werden.

Schauen wir uns die erscheinende Meldung etwas genauer an. Beim genauen Hinsehen ist ersichtlich, dass auch der Hintergrund im Web-Browser (hier Internet Explorer) läuft. Somit ist diese gefälscht, zeigt aber sehr schön, was mit etwas HTML-Kenntnissen möglich ist. Allenfalls wäre es auch aufgefallen, dass auf einem deutsch installierten Betriebssystem alle Meldungen auf Englisch erscheinen. Doch im ersten Schreckt fällt dies in der Regel nicht auf.

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21



Bildquelle: MSDN

Diese Art von Fehlermeldungen wird Scareware genannt: Scare (Schrecken) und ware von Software. Um an neue Opfer zu gelangen, versuchen die Betrüger die Suchergebnisse von Suchmaschinen zu beeinflussen. Dazu orientieren sie sich gezielt an Begriffen, welche häufig gesucht werden und erscheinen dann in den normalen Suchergebnissen relativ weit oben. Erst kürzlich hat Google seinen Suchindex (über 240 Millionen Einträge) durchsucht und dabei 11'000 verdächtige Webseiten gefunden, welche Scareware verbreiten.

Mit Scareware wird reales Geld verdient. Es geht diesen Leuten nicht um „Hacker-Kunst", sondern um den eigenen Profit. Da es hier um viel Geld geht, ist Scareware in der Regel hervorragend programmiert, auch wenn die Software schlussendlich keinen Mehrwert bietet.

Einmal installiert, ist es sehr aufwendig, diese wieder zu entfernen. Die Software klammert sich hartnäckig an den PC, oft sogar hartnäckiger als ein Wurm. Immer öfter geht Scareware gegen potentielle Gegner vor, schaltet Windows-Features und Schutzfunktionen aus.

Viele Antivirenprogramme haben Mühe, Scareware zu erkennen. Scareware kann sich sehr gut tarnen und somit vor den richtigen Antivirenprogrammen verstecken. Ein weiteres Problem ist, dass der betrügerische Akt ausserhalb der Software-Funktion liegt. Das Opfer zahlt ja freiwillig für diese Software. Die Vertriebsmethode ist das eigentliche Verbrechen. Auf der Software-Seite gibt es in der Regel keinen Unterschied zwischen einer schlechten Antivirensoftware, welche keine Viren entfernen kann und einer Scareware.

1.5 Spyware/Adware

Als Spyware wird üblicherweise Software bezeichnet, die persönliche Daten eines PC-Benutzers ohne dessen Wissen oder Zustimmung an den Hersteller der Software (Call Home) oder an Dritte sendet oder dazu genutzt wird, dem Benutzer direkt Produkte anzubieten.

Meist dienen Spywareprogramme dazu, das Surfverhalten im Internet zu analysieren. Die gewonnenen Daten werden kommerziell genutzt durch das Einblenden gezielter Werbebanner oder Pop-ups, die an die möglichen

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

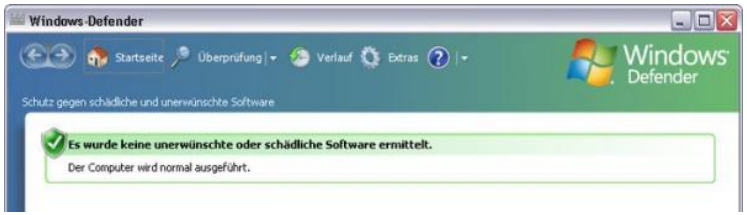
Interessen des Internetbenutzers angepasst sind. Die Unternehmen, die Spyware nutzen, erhoffen sich eine Steigerung der Wirksamkeit ihrer Werbemethoden.

Um mögliche juristische Probleme zu vermeiden, kennzeichnen viele Anti-Spyware-Programme die ermittelten Softwarekomponenten als möglicherweise unerwünschte Software (potentially unwanted software (PUS)).

Spyware wird meist für Unternehmen programmiert. Mitunter werden ganze Entwicklungsabteilungen damit beauftragt. Sie hat daher häufig ein sehr hohes technisches Niveau. Beispielsweise schützt sich Spyware gegen Löschung dadurch, dass mehrere Prozesse gleichzeitig laufen, die bei Beendigung sofort einen neuen Prozess starten und sich selbst kopieren. Auf der Festplatte entziehen sie dem Administrator die Schreib- und damit die Löschberechtigung.

Ein weiteres Problem entsteht dadurch, dass Spyware zusätzliche Sicherheitslöcher in einem System erzeugen kann, die dann sicherheitsrelevante Software-Updates verhindern.

Diese Verfahren machen es selbst technisch versierten Benutzern extrem schwer, sich der Spyware zu entledigen. Antivirensoftware-Hersteller haben Lösungen gegen Spyware entwickelt. Auch Microsoft hat dies erkannt und mit Windows Vista den Defender eingeführt, welcher vor Spyware warnt. Verfügbar ist das Programm auch für Windows XP.



1.6 Hoaxes

Hoaxes sind Unwahrheiten und ganzjährige Aprilscherze. Sie werden oft mittels E-Mail versandt und beinhalten häufig falsche Virenmeldungen. Solche Meldungen sollten einfach gelöscht werden!

Verschiedene Websites informieren über wahre und unwahre Virenmeldungen. Sehr empfehlenswert ist die Seite www.hoax-info.de der Technischen Universität Berlin.

1.7 Rootkits

Ein Rootkit ist eine Sammlung von Softwarewerkzeugen, die nach dem Einbruch in ein Computersystem auf dem kompromittierten System installiert wird, um zukünftige Logins des Eindringlings zu verbergen und Prozesse und Dateien zu verstecken.

- **Kernel-Rootkits**
  Kernel-Rootkits ersetzen Teile des Betriebssystemkerns durch eigenen Code, um sich selbst zu tarnen und dem Angreifer zusätzliche Funktionen zur Verfügung zu stellen, die nur im Kontext des Kernels ausgeführt werden können. Dies geschieht am häufigsten durch Nachladen von Kernelmodulen. Man nennt diese Klasse von Rootkits daher auch LKM-

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

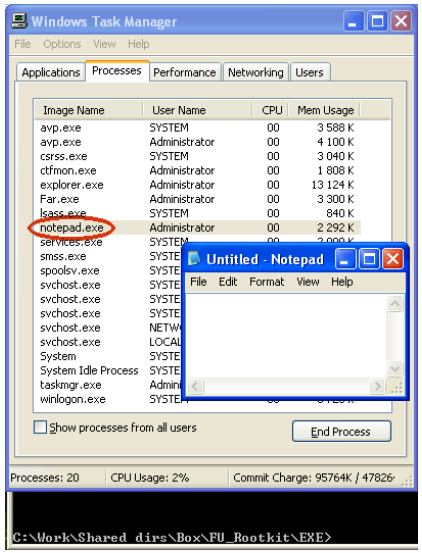
Telefon 052 320 91 20
Fax 052 320 91 21

Rootkits (LKM steht für engl. „loadable kernel module“). Einige Kernel-Rootkits kommen durch die direkte Manipulation von Kernelspeicher auch ohne LKM aus. Unter Windows werden Kernel-Rootkits häufig als neue .sys-Treiber realisiert.

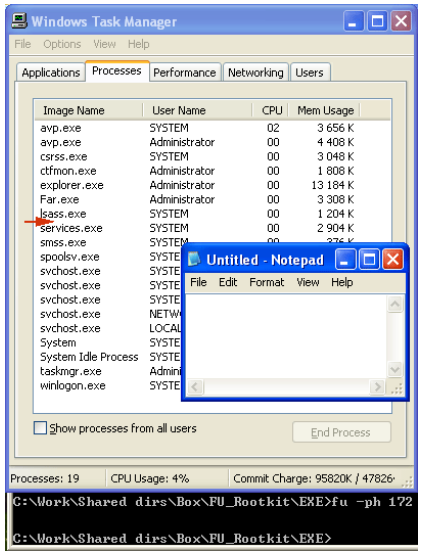
- **Speicher-Rootkits**
  Speicher-Rootkits existieren nur im Arbeitsspeicher. Nachdem das System neu gestartet wurde, sind diese nicht mehr vorhanden.

- **Userland-Rootkits**
  Userland-Rootkits sind vor allem unter Windows populär, da sie keinen Zugriff auf der Kernel-Ebene benötigen (daher der Name). Sie stellen eine DLL bereit, die mittels verschiedener Methoden direkt in alle Prozesse injiziert wird. Ist diese DLL einmal geladen, modifiziert sie entsprechende API-Funktionen und leitet die Ausführung dieser auf sich selbst um. Damit können Informationen gezielt gefiltert oder modifiziert werden.

Beispiel mit Notepad und dem FU-Rootkit:



Vorher



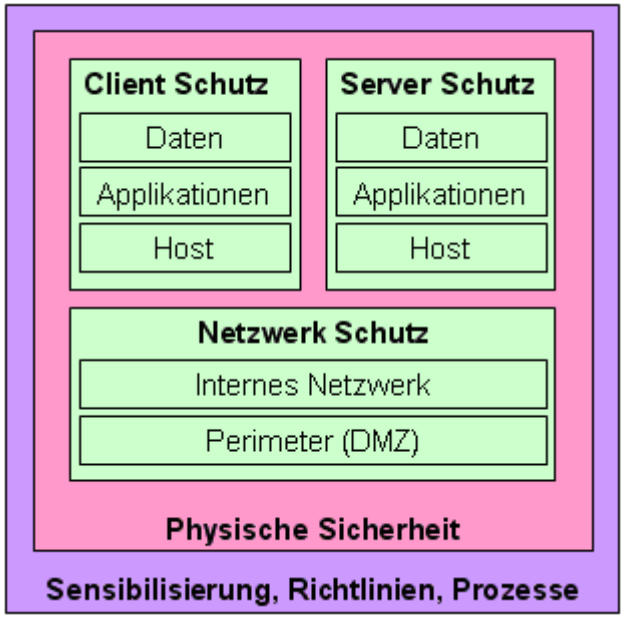
Nachher

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

2 Allgemeine Abwehr/Schutz



Die Abwehr- bzw. Schutzmassnahmen gegen Malware sollten mehrstufig sein. Nebst organisatorischen und personellen Massnahmen müssen Massnahmen im Netzwerk, auf den Server und den Clients getroffen werden.

2.1 Client Schutz

Client Schutzmassnahmen beziehen sich auf das Betriebssystem, die Applikationen und Daten. Sie setzen sich u.a. wie folgt zusammen:

- Angriffsfläche reduzieren
- Sicherheitspatches installieren
- Personal Firewall aktivieren
- Antiviren Software verwenden
- Richtlinie der „minimalen Rechte“ anwenden
- Anti-Malware Einstellungen vornehmen
- Massnahmen überprüfen und aktualisieren

2.2 Server Schutzmassnahmen

Server Schutzmassnahmen beziehen sich auf das Betriebssystem, die Applikationen und Daten. Sie setzen sich u.a. wie folgt zusammen:

- Angriffsfläche reduzieren
- Sicherheitspatches installieren
- Application Firewall aktivieren
- Funktionsspezifische Anti-Malware Einstellungen vornehmen
- Richtlinie der „minimalen Rechte“ anwenden
- Antivirensoftware verwenden
- Massnahmen überprüfen und aktualisieren

2.3 Netzwerk Schutzmassnahmen

Netzwerk Schutzmassnahmen beziehen sich auf das interne Netzwerk und die DMZ. Sie setzen sich u.a. wie folgt zusammen:

- Netzwerk Intrusion Detection System verwenden
- Application und URL Filtering verwenden
- Network Access Protection (NAP / NAC) einführen
- Quarantänen-Netzwerk zur Verfügung stellen
- Massnahmen überprüfen und aktualisieren

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

2.4 Physische Schutzmassnahmen

Die physischen Schutzmassnahmen beziehen sich vor allem Zutrittsmöglichkeiten. Nur Personen, die an Systeme müssen, dürfen auch an diese gelangen.

2.5 Personelle + organisatorische Massnahmen

Personelle und organisatorische Schutzmassnahmen umfassen u.a.

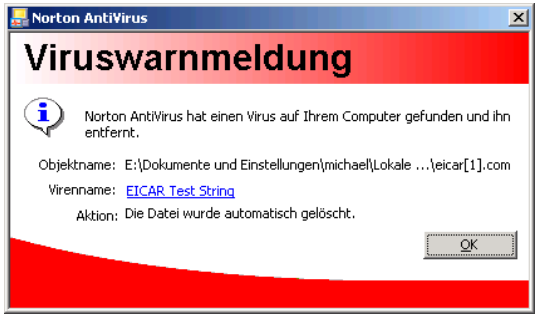
- Regelmässiges Backup und Überprüfung
- Regelmässiges Scannen
- Richtlinien für Laptops und Remoteuser
- Notfallkonzepte
- Awarenesskampagnen und Schulung von Usern und Administratoren
- usw.

2.6 Bestehende Massnahmen prüfen

Das Benutzerverhalten oder die Aktualität der eingesetzten Anti-Virenprodukte können mittels falscher, harmloser Viren überprüft werden. So kann zum Beispiel bei www.eicar.org folgende Fingerprint Datei herunter geladen werden:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Beim Herunterladen oder Öffnen von mit Viren-Fingerprints „verseuchten" Dateien sollte der Virenschutz der Arbeitsstation die Benutzeraktion mit einer Virenwarnmeldung abbrechen.



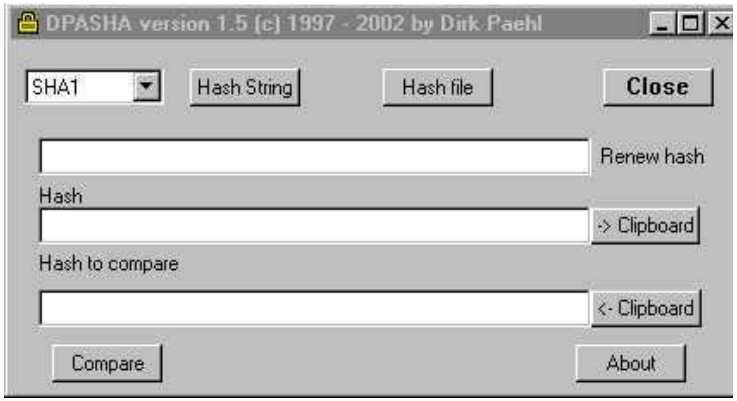
2.7 Hashwerte kontrollieren

Durch Viren veränderte Dateien oder Verzeichnisse werden leicht an einem neuen Hashwert erkannt. So können die Hashwerte von Original-Dateien mit den aktuellen Hashwerten verglichen werden. Sind die Hashwerte unterschiedlich, so wurde die Datei verändert. Verschiedene Programme helfen, die Hashwerte von Dateien, Verzeichnissen oder sogar Festplatten zu erstellen, zu verwalten und zu vergleichen. Die Software EnCase [http://www.guidancesoftware.com] wird beispielsweise von den Forensic-Ermittlern eingesetzt, um mit Hashwerten kompletter Systeme zu arbeiten oder das Freeware-tool DPASHA [http://www.paehl.de/cms/dpasha_deutsch] erlaubt die Hashwerte einzelner Dateien zu vergleichen.

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21



Weitere Schutzmassnahmen:

- Setzen Sie aktuelle Antiviren Produkte auf sämtlichen Rechnern ein.
- Halten Sie die Virendefinitionen immer auf dem neusten Stand.
- Sannen Sie in regelmässigen Abständen sämtliche Dateien auf Viren.
- Überprüfen Sie die ein- und ausgehenden E-Mails auf Viren.
- Filtern, bzw. löschen Sie automatisch die ausführbaren Dateien bereits auf dem Mailserver.
- Zeigen Sie alle Dateitypen an.
- Trainieren Sie den korrekten Umgang mit E-Mail-, Internet und Datenträger mit sämtlichen Benutzern.
- Sensibilisieren Sie die Benutzer auf die Gefahren durch Malware.
- Trainieren Sie mit den Benutzern die richtige Verwendung der Antiviren Tools.
- Testen Sie Ihre Benutzer und die eingesetzten Antiviren Produkte mit harmlosen „Viren-Fingerprint“-Dateien.
- Deaktivieren Sie das automatische Ausführen von Startmakros in den Anwendungen.
- Verzichten Sie auf die HTML-Darstellung von E-Mails in Mailclients.
- Überprüfen Sie regelmässig die Systeme auf ausgeführte Dienste, Prozesse, verfügbare Ressourcen und unübliche Aktivitäten.
- Erstellen und kontrollieren Sie Hashwerte z.B. von ausführbaren Dateien oder von Verzeichnissen.
- Setzen Sie nur Lese-Berechtigung auf die ausführbaren Dateien.
- Starten und öffnen Sie keine Dateien als Administrator.
- Verwenden Sie ausschliesslich Originalsoftware. Seien Sie besonders vorsichtig bei Free- und Shareware
- Aktivieren Sie die möglicherweise im BIOS vorhandene Virenschutzfunktion.
- Backup, Backup, Backup!

3 Malware Zukunft

Kaspersky Lab prognostiziert eine in Zukunft weiter steigende Professionalisierung der Cybercrime-Szene. Genau wie in herkömmlichen Industriezweigen hat sich mittlerweile eine ähnlich strukturierte Untergrundindustrie gebildet. Wenn zunehmend über mobile Geräte auf das Internet zugegriffen wird, und auch immer häufiger sensible Aktionen wie Online-Banking über Smartphones getätigt

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

werden, wird sich auch die Malware-Landschaft dementsprechend ändern. Der IT-Sicherheitsexperte geht daher davon aus, dass es in Zukunft verstärkt Attacken auf mobile Anwender geben wird. Laut Eugene Kaspersky, CEO und Mitgründer von Kaspersky Lab, sind mobile Attacken in der Regel einfach zu realisieren. Denn mobile Anwender sind ständig mit dem Internet verbunden. Daher nimmt Kaspersky Lab an, dass in Zukunft für mobile Geräte dieselben Risiken bestehen wie aktuell für herkömmliche PCs.

Daher stellt sich die Frage, ob sich der Anti-Virenschutz bald gänzlich ins Internet verlagert. Eine lokale Virendatenbank und ihre ständige Aktualisierung seien bei durchschnittlich 2'500 neuen Schädlingen am Tag nicht mehr zeitgemäss, so Raimund Genes, CTO Anti-Malware bei Trend Micro. Mithilfe von „in the Cloud Services" oder „Security as a Service" liesse sich das Problem der ständigen Aktualisierung und der damit verbundenen Hardware-Kapazität lösen. Die Experten von F-Secure kommen zum Ergebnis, dass die Anzahl der Schadprogramme bis zum Jahresende wohl auf rund eine Million anwachsen wird – basierend auf den Berechnungen des ersten Quartals 2011.

Bis aber Dienste zur Malware-Bekämpfung umfassend ins Internet verlagert werden, dauert es sicherlich noch einen Moment. Jedoch gilt es, den Malwareschutz jederzeit sicherzustellen. Dazu gehören auch regelmässige Kontrollen bei Servern und Clients.

4 Quellen

- IT-Security Engineer, Klubschule Migros, Michael Achermann
- Teilweise Ausschnitte aus Wikipedia, der freien Enzyklopädie
- Kompendium E-Mail-Security von SearchSecurity.de

Bild: paid4magazin.de