

Network Security Taskmanager

Neue Technologie für sichere Netzwerke

- + Aufspüren von bisher nicht erkennbaren Schädlingen
 - + Analyse und Klassifizierung von Prozessen
 - + Zentrale Administration und Auswertung
-

= Erweiterter Schutz für Ihr Netzwerk

Warum?

Ist Zustand

- Stets aktuelle Updates, Antivirus, Firewall
- User arbeiten mit eingeschränkten Benutzerrechten
- Sicherheitsrichtlinien

Aber:

- Auch bei einem eingeschränkten Benutzer ohne Installationsbefugnis kann ein Angreifer per exploit erweiterte Rechte erlangen oder Schadsoftware ausführen.
- Dass selbst kurze Update-Intervalle und Erkennungsraten über 99% einen Computer nicht ausreichend schützen können, verdeutlichte die c't aus dem Heise Verlag anhand eines kleinen Rechenbeispiel. Selbst wenn der AV-Hersteller innerhalb 1h nach Auftauchen eines neuen Schädlings passende Signaturen bereitstellt und diese sofort eingepflegt werden, können mit einem kleine bot-Netz in dieser Zeit 10. Mio Computer infiziert werden.

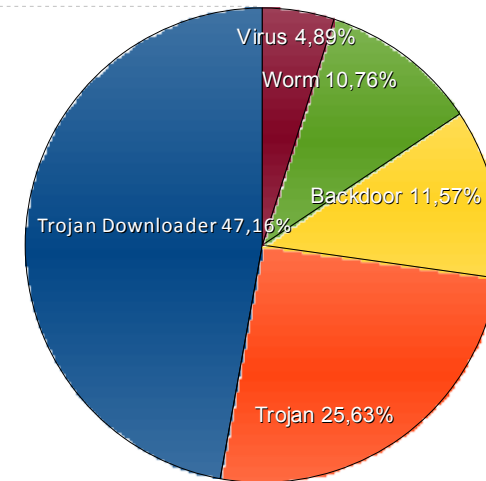
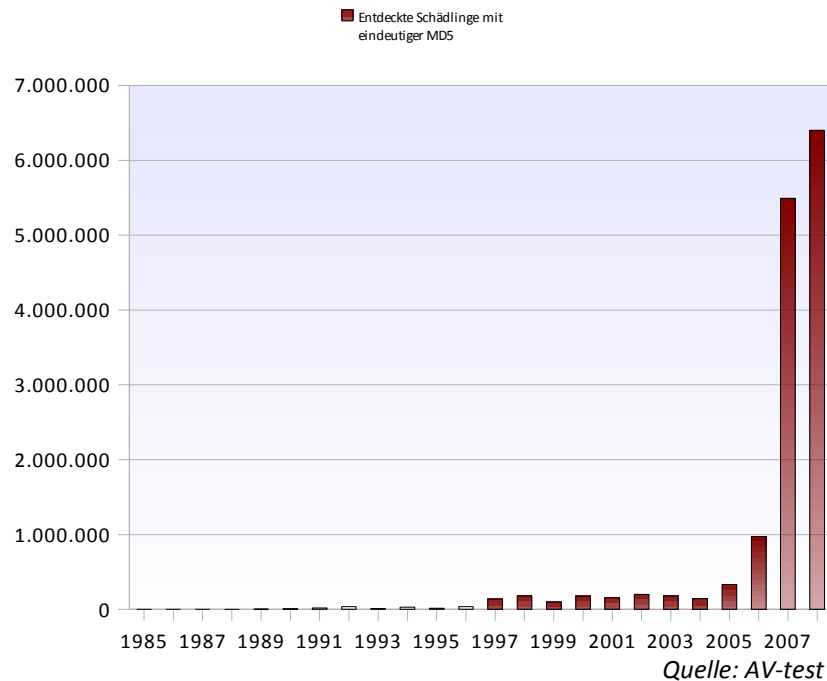
Problem

Veränderte Sicherheitslage

- Gezielte Angriffe (statt wie früher Viren und Spyware)
- Ausgefeilte Angriffstechnik
- Attacken auf Firmennetze finden permanent statt
- Professionalisierung und Kommerzialisierung

Wie professionell ein gezielter Angriff gegen eine Behörde aussehen kann, zeigt ein Fall vom Mai 2008: 500 Mitarbeiter der Schweizer Bundesverwaltung erhielten eine email, die zum Anklicken von Bildern verleite. Wer auf das Bild klickte, installierte einen Bildschirmschoner, der einen Trojaner enthielt, welcher Spionage-Programme nachlädt. Die email selbst sah absolut vertrauenswürdig aus: korrekte Anrede mit Namen, Bundesstelle als Absender, die Bilder lagen auf einer gut gemachte Kopie eines Bundesstellen-Servers. Die eingesetzte Malware wurde damals durch keine gängige Antiviren-Software erkannt. Eine Analyse des Angriffs zeigte, dass die Täter sehr professionell vorgingen und finanziell und technisch bestens ausgerüstet waren.

Wachsende Anzahl von Schädlingen



Symantec-Chef John Thompson schätzt, dass 2008 erstmals mehr Schadsoftware als gutartige Software programmiert wird. Angesichts solcher Zahlen, ist es verständlich, wenn Eugen Kaspersky meint, dass die gesamte Sicherheitsbranche dieser Flut irgendwann nicht mehr standhalten könnte. Und McAfee Chef Dave De Walt sagte im Sommer 2008, das jetzige signaturbasierte Blacklisting Prinzip wird technisch nicht mehr machbar sein.

79 % aller Malware kann man sich durch den Besuch von vertrauenswürdigen Seiten einfangen.

Verbreitung von Malware

- Email Anhang hat ausgedient (1 von 200 emails)

- Drive-by-Download

Per XSS oder SQL-Injection wird schädlicher JavaScript Code oder Iframe in bestehende Webseiten eingeschleust. Der Besuch einer solchen Webseite reicht, um Malware downzuloaden und zu starten.

- täglich 20.00 neue präparierte Webseiten
 - davon sind 79% vertrauenswürdige Webseiten (ARD, Verisign, Trend Micro, McAfee)
- Social Engineering
 - Suchmaschinen Eintrag (IKEA, Juni 2008)
 - persönliche email (Anrede, bekannte Namen/Orte/Fragen)

Beispiel **Social Engineering**: Wer im Sommer 2008 bei Google nach ikea gesucht hatte und auf den ersten Link klickte ...

The screenshot shows a Mozilla Firefox browser window titled "ikea - Google-Suche - Mozilla Firefox". The address bar contains "http://www.google.de". The search bar has "ikea" entered, and the search button is labeled "Suche". Below the search bar, there are radio buttons for "Suche: Das Web" (selected), "Seiten auf Deutsch", and "Seiten aus Deutschland".

The search results are displayed under the heading "Web". The first result is highlighted in yellow and is an advertisement for "IKEA Einrichtungshaus" from "www.IKEA.com". The text of the ad says "Das nächste IKEA Einrichtungshaus findest du direkt hier." and includes an "Anzeige" label on the right.

The second result is "IKEA | Startseite" with a description: "Geschichte und Idee der Gründung sowie natürlich viele Infos zu den Möbeln und Geschäften." It includes the URL "www.ikea.com/de/de/" and statistics "- 33k - Im Cache - Ähnliche Seiten".

The third result is "Welcome to IKEA.com" with a link to "[Diese Seite übersetzen]". The description says "Featuring Scandinavian modern style furniture and accessories. Include storage options, lighting, decor products, kitchen appliances and pet care." It includes the URL "www.ikea.com/" and statistics "- 22k - Im Cache - Ähnliche Seiten". A link "Weitere Ergebnisse von www.ikea.com »" is also present.

The fourth result is "Ikea – Wikipedia" with a description: "Ikea (Handelsmarke: IKEA) ist ein multinationaler Einrichtungskonzern. Das Unternehmen wurde 1943 von Ingvar Kamprad in Schweden gegründet und gehört heute ...". It includes the URL "de.wikipedia.org/wiki/Ikea" and statistics "- 72k - Im Cache - Ähnliche Seiten".

The fifth result is "IKEA Möbel: Wohnideen + IKEA Katalog - StyleSpion" with a description: "7. Aug. 2007 ... IKEA: Für viele Leute ist er nicht einfach nur ein Katalog. Nein, die jährlich im Sommer erscheinende Warenschau des Möbelherstellers ist ...". It includes the URL "stylespion.de/ikea-moebel-wohneideen-katalog/855/" and statistics "- 41k - Im Cache - Ähnliche Seiten".

The sixth result is "homepage - IKEA Group" with a link to "[Diese Seite übersetzen]".

At the bottom of the browser window, the status bar shows "Fertig" and a small icon.

... landete auf eine nachgemachte Webseite, die Schadsoftware installiert.

The screenshot shows the IKEA Germany homepage. At the top, the IKEA logo is on the left, and navigation links for 'Onlineshop', 'Zum Warenkorb', and 'IKEA Service' are in the center. On the right, there are links for 'Mein Profil/Anmelden', 'IKEA in deiner Nähe', 'IKEA FAMILY', and 'jobs@IKEA'. A search bar is also present. Below the navigation, a yellow banner lists various product categories like 'Alle Produkte', 'IKEA Neuheiten', 'Küche', 'Wohnzimmer', etc. The main banner features the text 'SOMMER BEI IKEA' and 'Ein Besuch bei IKEA und du bist bereit für die Sommerferien'. A blue error dialog box is overlaid in the center, with the title 'Webseiten Plugin nicht gefunden' and the message: 'Bitte laden Sie sich das Plug herunter um diese Webseite richtig darstellen zu können. Klicken Sie auf OK um den download zu starten.' Below the dialog, there are five promotional tiles: 'Einkaufsmöglichkeiten' (with links to Onlineshop, delivery conditions, and A-Z products), 'Für sonnige Gemüter' (promoting a sun umbrella), 'Aufräumen & Organisieren' (promoting storage solutions), 'Schlafzimmer' (promoting bedroom ideas), and 'IKEA in deiner Nähe' (promoting local offers and a map of Germany).

Weil hier der User selbst den Download startet und das vermeintliche Plugin installiert, blockieren Firewall und andere Sicherheitsprogramme die Schadsoftware nicht.

Gezielte Angriffe

Ziel eines solchen Angriffs sind Informationen, Adressen, Projekte, Zugangsdaten, ...

Die Motivation der professionell organisierten Täter ist hauptsächlich finanzieller Natur.

Eine technisch anspruchsvolle Malware nutzt aktuelle Schwachstellen in Standard-Anwendungen, um sich zu installieren oder um weitere Rechte zu erlangen.

z.B. PDF Exploit: Beim Öffnen der PDF-Datei wird ein eingebettetes Schadprogramm ausgeführt. Auch Antiviren-Produkte werden als Einfallstor mißbraucht, da Angreifer voraussetzen können, dass diese in Netzwerken vorhanden sind.

Hacker testen im Vorfeld einen gezielten Angriff mit allen bekannten Sicherheitslösungen und modifizieren solange, bis sie 100%ig sicher sind, dass die Malware nicht erkannt wird. Da nur wenige Samples einer solchen angepassten Malware im Umlauf gelangen, besteht kaum ein Chance, dass diese jemals in den Antiviren-Signaturen integriert werden.

Angriffspunkt: Arbeitsplatz Rechner

- Internet ist bevorzugter Weg für Angriffe
- Server gut abgesichert und überwacht
- **aber:** Schwachstelle Mensch
- **aber:** Jeder Arbeitsplatz Rechner ist gefährdet für maßgeschneiderte Malware

Lösung

Network Security Taskmanager

- Erkennt maßgeschneiderte oder neuartige Schadsoftware auf den Computern im Netzwerk
- Nicht signaturbasiert
- Zentrale Auswertung
- Verhaltens- und Prozess-Analyse

Network Security Taskmanager

Datei Bearbeiten Ansicht Hilfe

Zurück Logbuch Computer hinzufügen Online Info

Computername eingeben

Aktueller Netzwerk Sicherheitsstatus

Hier sehen Sie alle potenziell gefährlichen Prozesse, die bei den letzten Scans aktiv waren. Regelmäßige Scans per Zeitplanung erhöhen die Aktualität dieser Übersicht.

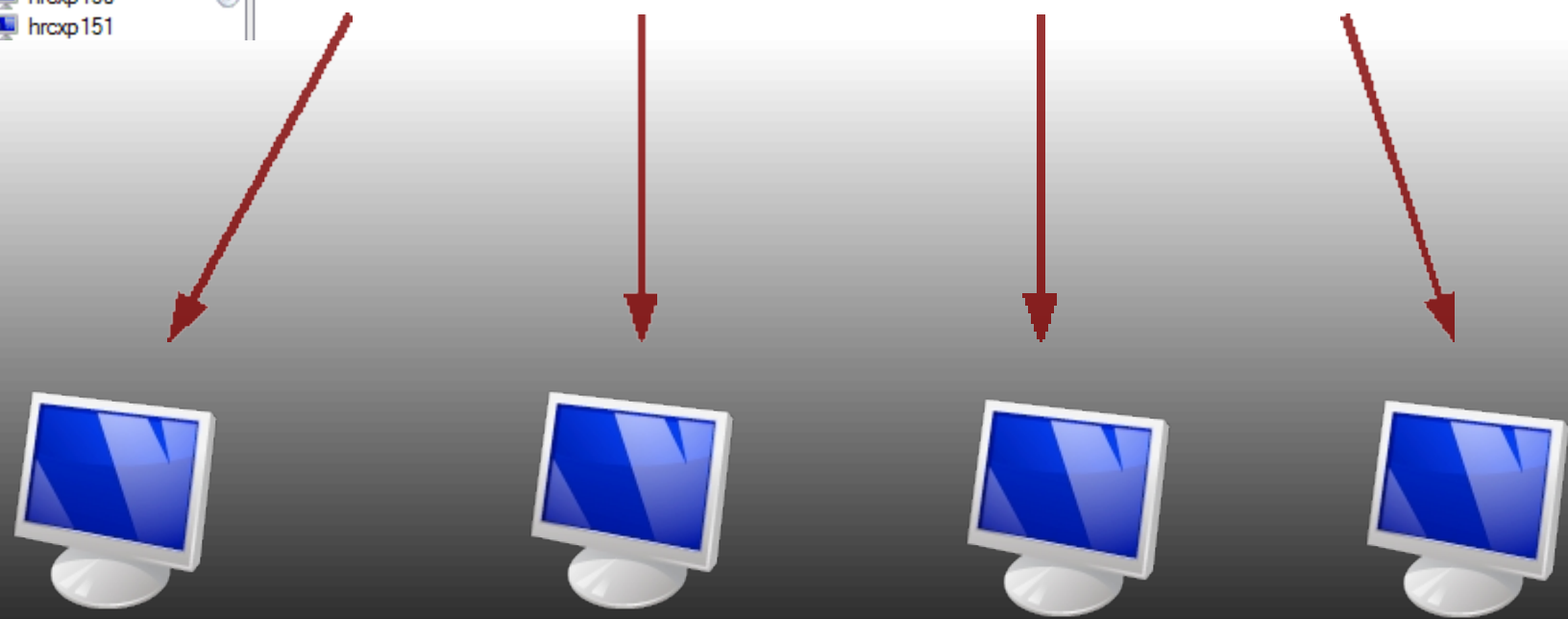
Name	Bewertung	RAM	Beschreibung	Hersteller	Läuft auf	Datei
Mpk.exe	89	2,0 MB		-	cvmxp-28	C:\Programn
DameWare Mini Remote...	64	3,1 MB	A component of the Dame...	DameWare Development L...	cvmxp-22	C:\Windows
spicetray_silent.exe	36		Spiceworks	Spiceworks	wswin2000	C:\Programn
Java Update Scheduler	34	1,7 MB	Java(TM) 2 Platform Stand...	Sun Microsystems, Inc. : Ja...	hnpc2, cvm...	H:\Programr
CTF Loader	20	0,4 MB		Microsoft Corporation : Micr...	cvmxp-28	C:\Windows
spicetray		0,3 MB	GDI+ Window, Spiceworks...	Spiceworks, Inc. : Spicewo...	cvmxp-28	C:\Programn
DebugView		0,4 MB	DebugView on \\CVMXP-2...	Microsoft Corporation : Sysi...	Vetra009	C:\Dokumer

Administration

- Status
- Konfiguration
- Referenzdatenbank

Computer

- < Neue Gruppe >
- Finanzabteilung
- 141.30.87.112
- achill140
- achill143
- cvmxp-22
- cvmxp-23
- cvmxp-28
- hnpc2
- hrcxp 150
- hrcxp 151



Ressourcenschonend & Sicher

- Netzwerk Traffic:
 - 50 KB je Client (300 Prozesse inkl. alles)
- Speicherung aller Daten auf Server
 - 100 KB je Client
- Speicherplatz auf Client
 - 250 KB Agent + 1 MB temporäre Daten
- CPU schonend durch optimiertes Threadpooling
- Höchste Sicherheit
 - AES 128 Bit, signiert
 - Sicherer Schlüsselaustausch, Sessionkeys

Wie wird der Admin gewarnt?

Auffälliger Prozess auf CVXP-27 - Network Security Task Manager

Auf Computer "CVXP-27" wurde ein unbekannter auffälliger Prozess gefunden.

xhack logger
Datei: C:\WINDOWS\sysxha32.exe
Gefährlich: 72%
ProcessID: 171

Hier klicken um diesen genauer anzusehen.

12:48



Aktueller Netzwerk Sicherheitsstatus

Hier sehen Sie alle potenziell gefährlichen Prozesse, die bei den letzten Scans aktiv waren. Regelmäßige Scans per Zeitplanung erhöhen die Aktualität dieser Übersicht.

Name	Bewertung	Beschreibung	Hersteller	Läuft auf
MPK.exe	89	Mini Remote Control	-	vxp-23
DameWare Remote	64	A component of ...	DameWare Dev	vmxp-28

Nicht angezeigt wird der auffällige Prozess "no.exe" der nach dem angezeigten Scan aktiv war.

Fehler- und Auffälligkeiten

Filter

Web Info Client Ereignisse

Technische Fehler Auffällige Prozesse

Folgende auffällige Prozesse wurden bisher gefunden.

Wertung	Max.	Name	Datei	Computer	Zeit
74%		spiceworks.exe	C:\Programme\Spice\spice.exe	cvmxp-28	20.
89%		MPK.exe	C:\Programme\KGB\MPK.exe	cvmxp-28	20.
100%		Port Reporter	H:\Programme\Port\portrep.exe	hnpc2	20.

Alle auffälligen Prozesse anzeigen

Exportieren... Schließen

Ereignisanzeige

Datei Aktion Ansicht ?

Ereignisanzeige Anwendung 427 Ereignis(se)

Typ	Quelle	Kategorie	Ereignis
Warnung	NetTaskAgent	(10054)	150

Wie wird der Admin gewarnt?

Ereignisanzeige in System-Management-Software

- HP OpenView
- IBM Tivoli
- CA Unicenter
- Microsoft System Center Operations Manager (MOM)
- Nagios

Vergleich

	Antivirus	NetSTM	IDS	Whitelist
Einrichtung	○	⊕	○	○
Wartung	⊕	⊕	⊖	⊖
bekannte 👁	⊕	○	○	⊕
unbekannte 👁	⊖	⊕	○	⊕

- ⊕ einfach
- Hintergrundwissen erforderlich
- ⊖ geschulter Administrator erforderlich

Nachteile

Network Security Taskmanager

- Fehlalarm/unscharfe Ergebnisse möglich
- Ruhender Schädling wird harmloser bewertet
- Jedes Programm kann auch Angriffsziel sein
- Notwendige Prozesse und damit Client abschließbar
(deswegen extra Bestätigung bei Prozess beenden)

Rechtliche Aspekte / Datenschutz

Network Security Taskmanager dient nicht zur Überwachung von Mitarbeitern.
Es ist nicht möglich, das Verhalten von Mitarbeitern aufzuzeichnen.

Network Security Taskmanager wird im Rahmen der Netz- und Systemanalyse eingesetzt.
Die Software hilft Wirtschaftsspionage, Sabotage und sicherheitskritische Software aufzudecken.

Die Geschäftsleitung ist gesetzlich (KonTraG) verpflichtet, Systeme und Software einzurichten, "damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden". Wird dies unterlassen, können Vorstände oder Geschäftsführer persönlich haftbar gemacht werden.

Keine personenbezogenen Daten

Die Aufzeichnung von aktiven Prozessen erfolgt nur in dem Umfang, wie es für die Erkennung von Angriffen, Angriffsversuchen und Sicherheitsverletzungen und deren Rückverfolgung erforderlich ist. Daten werden zu keinem anderen Zweck aufgezeichnet.

Wie bei anderer Sicherheitssoftware auch, sollte der Betriebs- bzw. Personalrat informiert werden.

Zusammenfassung

Network Security Taskmanager

- Erkennt Malware, die von bisherigen Sicherheitslösungen nicht erkannt wird
- Zusammen mit dem **BSI** entwickelt
- Zentrale Verwaltung
- Erprobt: Security Task Manager
schützt tausende Computer weltweit
- Einfache und schnelle Installation
- Läuft parallel zu jeder anderen Sicherheitssoftware