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.

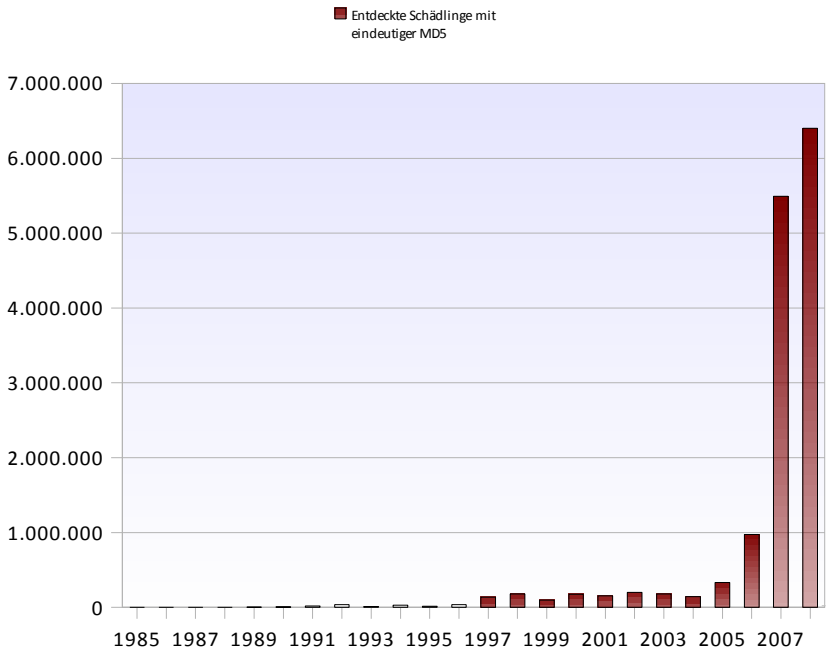
Problem

Veränderte Sicherheitslage

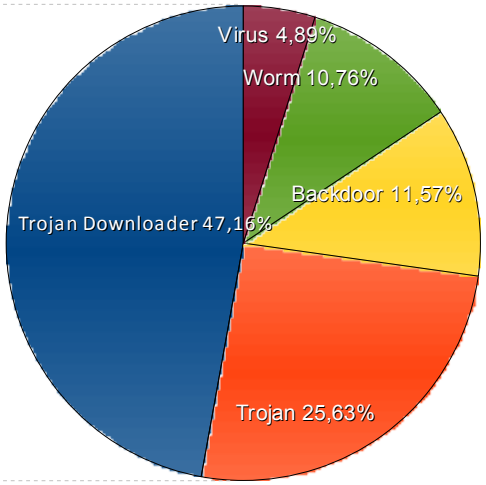
- Gezielte Angriffe (statt wie früher Viren und Spyware)
- Ausgefeilte Angriffstechnik
- Attacken auf Firmennetze finden permanent statt
- Professionalisierung und Kommerzialisierung

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



Quelle: AV-test



Quelle: Microsoft

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.

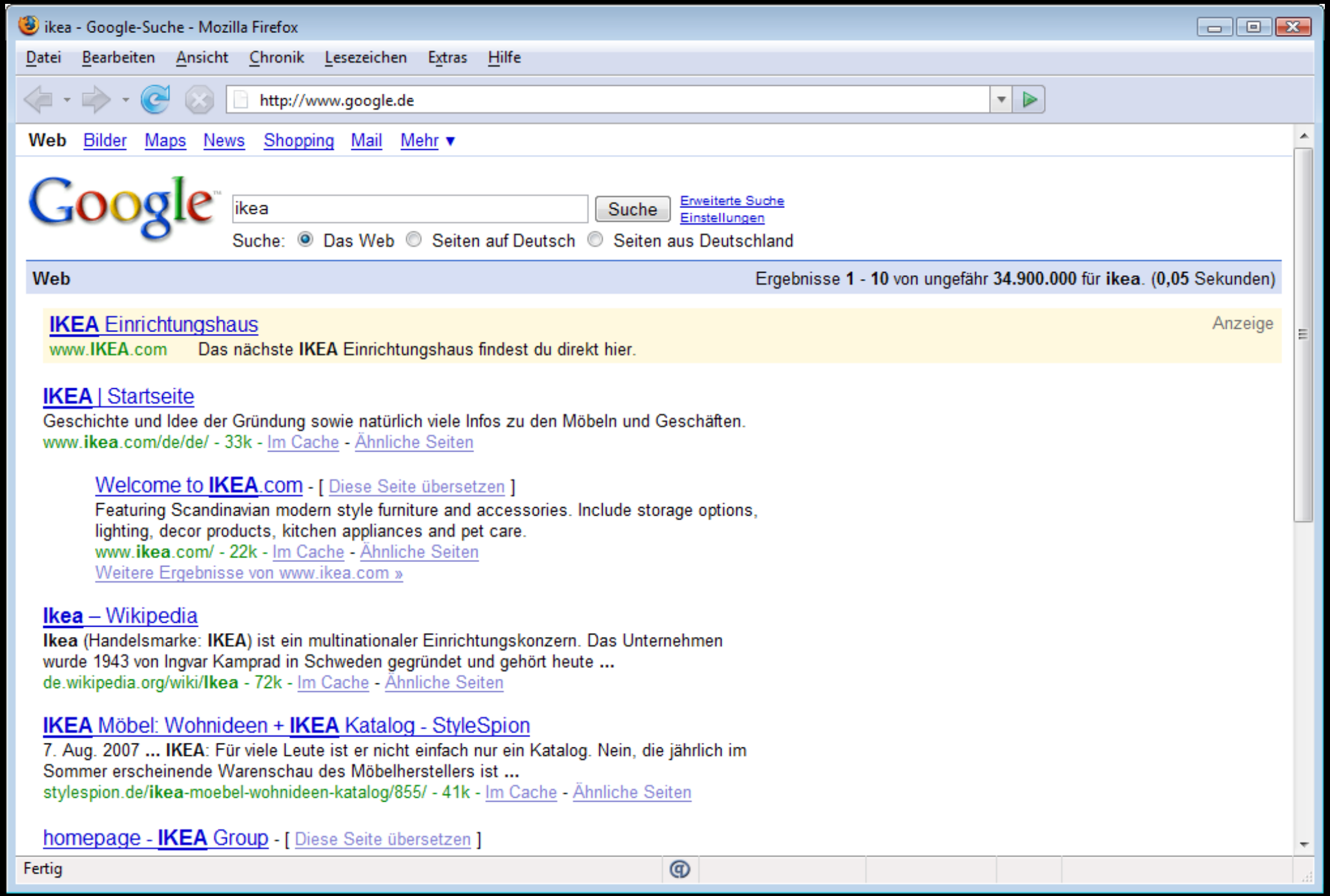
http://www.neuber.com/network-taskmanager/

Verbreitung von Malware

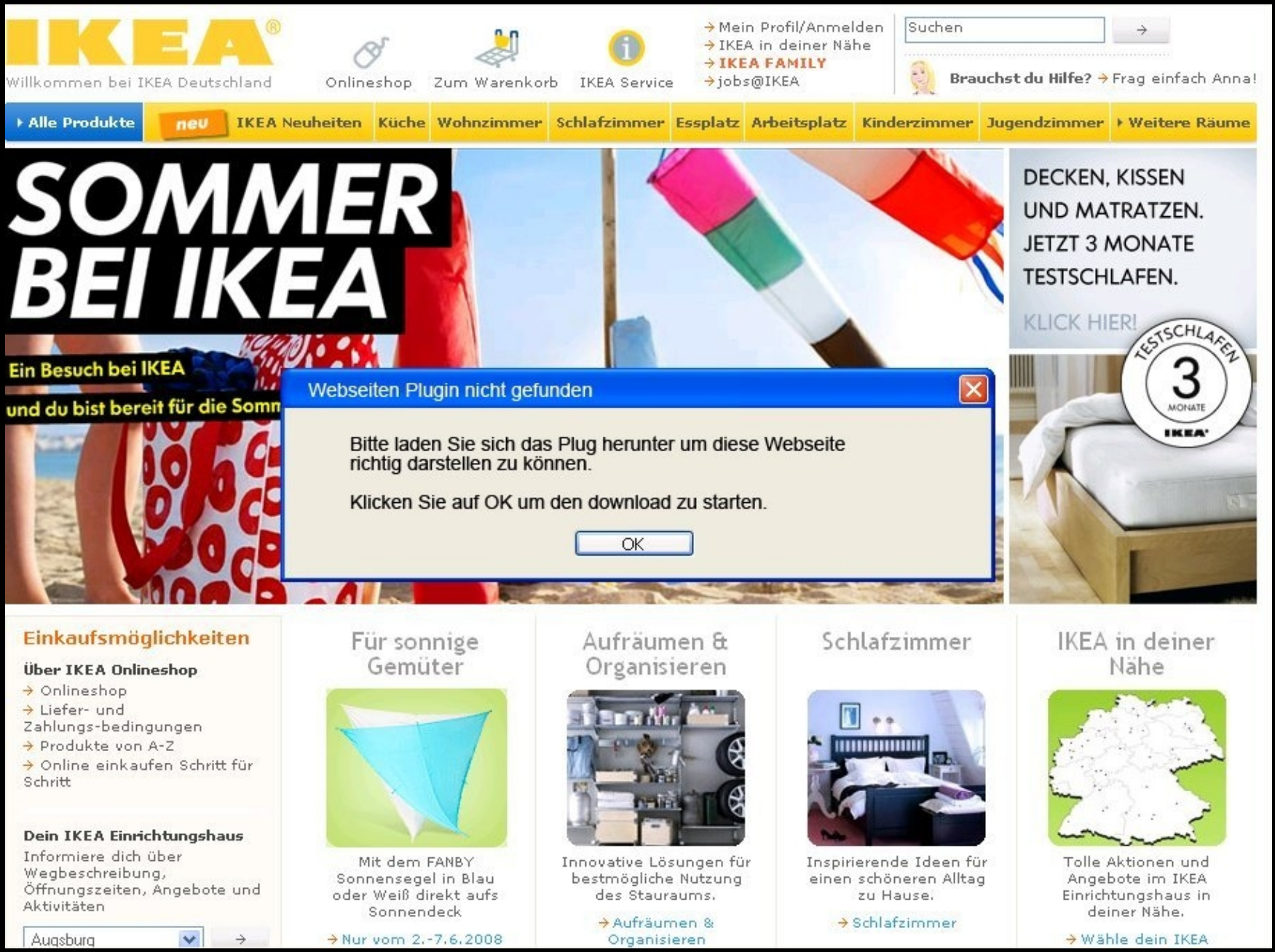
- Email Anhang hat ausgedient (1 von 200 emails)
- Drive-by-Download

  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 präperierte 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 ...



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



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 erweitere Rechte zu erlangen.
z.B. PDF Exploit: Beim Öffnen der PDF-Datei wird ein eingebettes Schadprogramm ausgeführt.
Auch Antivieren-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

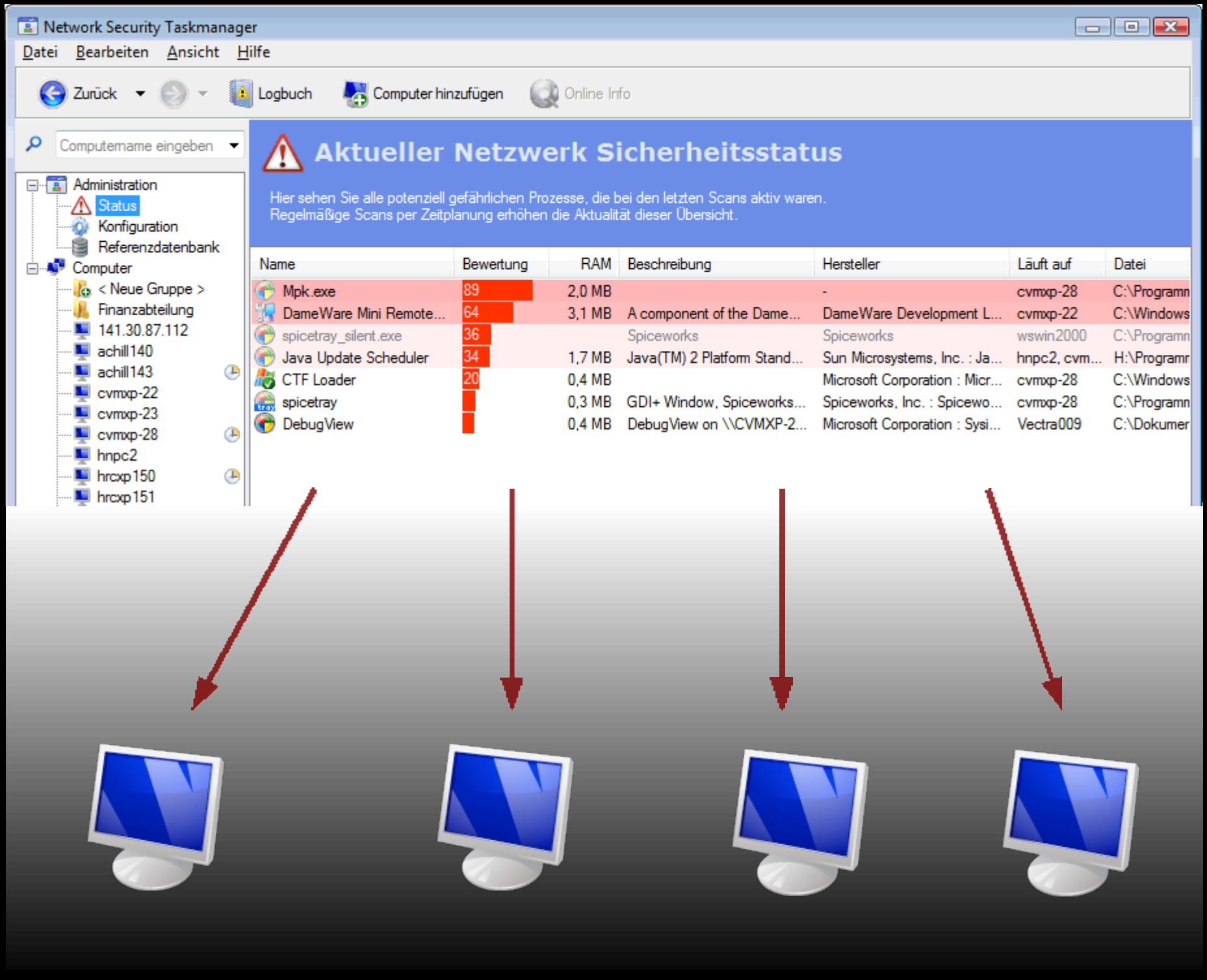
- Internet ist bevorzugter Weg für Angriffe
- Server gut abgesichtert und überwacht
- aber: Schwachstelle Mensch
- aber: Jeder Arbeitsplatz Rechner ist gefährdet
  für maßgeschneiderte Malware

http://www.neuber.com/network-taskmanager/

Lösung

Network Security Taskmanager

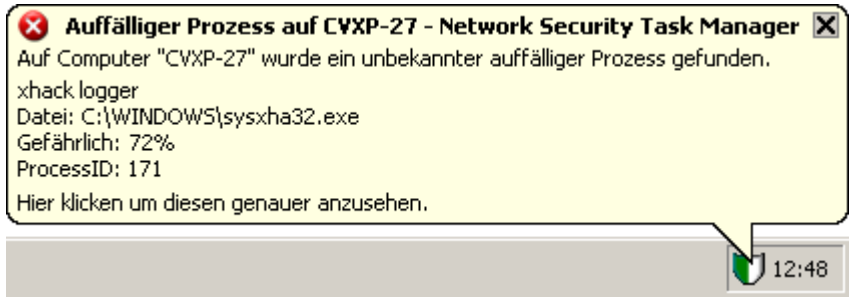
- Erkennt maßgeschneiderte oder neuartige Schadsoftware auf den Computern im Netzwerk
- Nicht signaturbasiert
- Zentrale Auswertung
- Verhaltens- und Prozess-Analyse

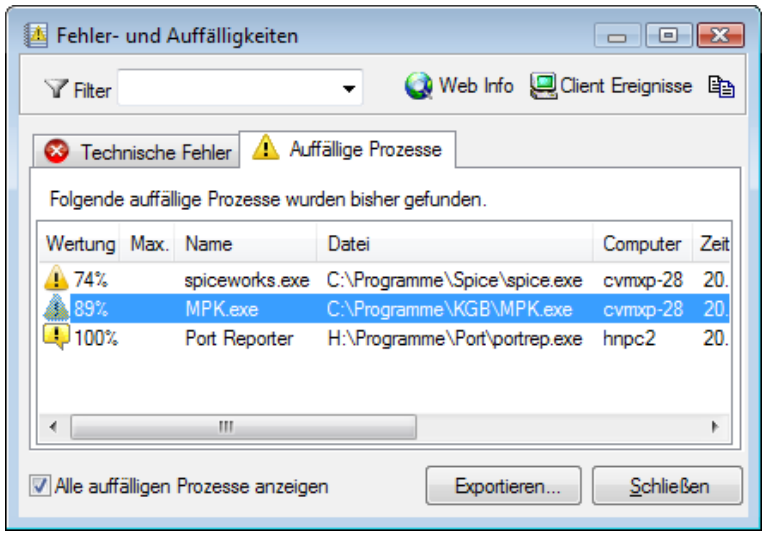

Network Security Taskmanager
Datei Bearbeiten Ansicht Hilfe
Zurück
Logbuch
Computer hinzufügen
Online Info
Computername eingeben
Administration
Status
Konfiguration
Referenzdatenbank
Computer
< Neue Gruppe >
Finanzabteilung
141.30.87.112
achill140
achill143
cvmxp-22
cvmxp-23
cvmxp-28
hnpc2
hrcxp150
hrcxp151
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... Vectra009 C:\Dokumer

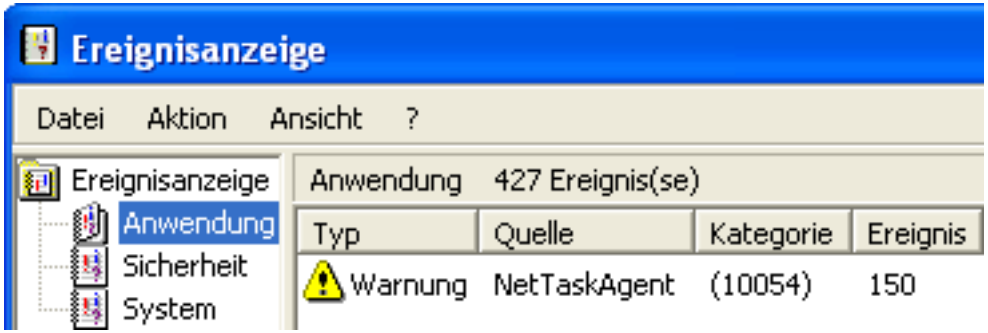
Ressourcenschonend & Sicher

- 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?







http://www.neuber.com/network-taskmanager/

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 abschießbar
  (deswegen extra Bestätigung bei Prozess beenden)

http://www.neuber.com/network-taskmanager/

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 personenbezogen 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

http://www.neuber.com/network-taskmanager/