Viren, Würmer und Trojaner

Weiterbildungsveranstaltung des PING e.V.

Daniel Borgmann
und
Dr. med. Arthur Pranada

Dienstag, 12. Dezember 2006

Viren, Würmer und Trojaner

Virenlawine ...

news 17.05.2005 12:08

WM-Wurm Sober.O ist Auslöser der Spam-Welle

Die Vermutung über den Zusammenhang zwischen dem **WM-Ticket-Wurm Sober.O[1]** und der **Welle von Mails mit teilweise rechtsgerichtetem Inhalt[2]** hat sich bestätigt. So stoppte Sober.O Mitte der letzten Woche seine eigene Verbreitungsroutine, um infizierte Windows-PCs zu Spam-Bots umzufunktionieren. Dazu lud er von diversen Servern ein Programm nach, das die Hersteller von Antivirensoftware Sober.P getauft haben. Sober.P startete dann am vergangenen Samstag den Versand von Mails in großem Umfang mit gefälschter Absenderadresse.

FAZ 2003-06-06
Computer
Virenlawine durch "Bugbear.B"
"Bugbear.B" ist wie sein Vorgänger "Bugbear" auf Pin-Nummern von Kreditkarten und Paßwörter aus. Die neue Variante des Computervirus vereint ...

FAZ 2003-08-22
Sobig.F schlägt alle Rekorde
Der schnellste Computerwurm
HAMBURG, 21. August (dpa). Der erstmals am Dienstag in Umlauf gebrachte neue E-Mail-Wurm Sobig.F hat am Donnerstag einen Geschwindigkeitsrekord ...

FAZ 2004-06-04
Computer
Neuer PC-Wurm stiehlt Paßwörter fürs Online-Banking
Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt vor einem neuen Computerwurm. Besonders brisant: "Korgo", so der Name des ...

FAZ 2004-06-05
Der Computerwurm Sasser legt Millionen Rechner lahm
Urheber vermutlich in Rußland / Viren werden immer schneller entwickelt / Von Holger Schmidt
FRANKFURT, 5. Mai. Stundenlange Verspätungen bei British Airways, eine lahmgelegte Küstenwache und Handbetrieb an den Postschaltern: Der Computerwurm ...

Viren, Würmer und Trojaner

news 22.11.2005 09:23

Neuer Sober-Wurm tarnt sich als Mail des Bundeskriminalamts

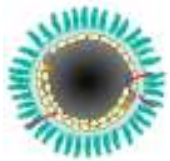
Kaum ist die letzte Sober-Welle abgeklungen, tritt eine neue Variante auf den Plan und versucht, die Windows-Systeme von Anwendern zu infizieren. Anders als bei seinen **Vorgängern Sober.V/.W[1]** sind die Nachrichtentexte von Sober.Y/.Z sehr viel raffinierter. Unter anderem tarnt sich der

Übersicht

- Was ist ein Virus?
- Wie fing das alles an?
- Wie viele Viren gibt es heute eigentlich?
- Wie kann sich mein Computer infizieren?
- Wie funktionieren Viren?
- Können Viren Schäden anrichten?
- Wie kann ich mich schützen?
- Was bringt die Zukunft?

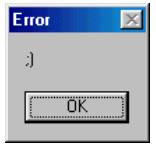
Viren, Würmer und Trojaner

Was ist ein Virus?



Viren in der Medizin

- das Virus
  - *lat. / Sanskrit:* Schleim oder Gift
- Definition
  - obligat intrazelluläre Parasiten (= müssen in einer Zelle leben)
  - Vermehrung: nicht selbständig, nur durch Wirte
  - Eigenschaften: Verändern Erbgut



Computerviren

- Computerprogramm
  - mit Verbreitungs- und Infektionsfunktion
- Definition
  - Benötigt/infiziert andere (harmlose) Programme und nutzt diese als Wirt
  - Vermehrung: durch das Wirtsprogramm
  - Eigenschaften: Verändern Programmcode

Definition Computer-Viren, Würmer und Trojaner

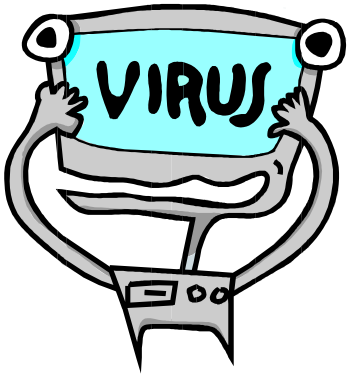
- Ein Virus ist ein Programm, das sich verbreitet, indem es andere (harmlose) Programme benutzt.
- Ein Wurm ist ein Programm, das sich eigenständig verbreitet.
- Ein Trojaner ist ein Programm, das sich als harmloses Programm tarnt.

Wie fing das alles an?

- 1982
  - Der 15-jährige Rich Skentra stellt ein Programm vor, das sich auf Apple-II-Rechnern verbreitet und bei jedem 50. Mal ein Gedicht präsentiert
- 10. November 1983
  - Fred Cohen stellt erstes Computervirus vor
  - für Betriebssystem Unix
  - Teil einer Forschungsarbeit / Doktorarbeit: „Programme, die andere Programme infizieren indem sie diese verändern um möglicherweise eine verbesserte Version von sich selbst einzubauen"
- 19. Januar 1986
  - Der erste Bootsektor-Virus für das Betriebssystem MS-DOS gelangt in die Freiheit
  - Entwickelt von Basit und Amjad Alvi aus Lahore, Pakistan
  - Copyright-Hinweis auf Disketten beim Kopieren

Wie viele Viren gibt es heute eigentlich?

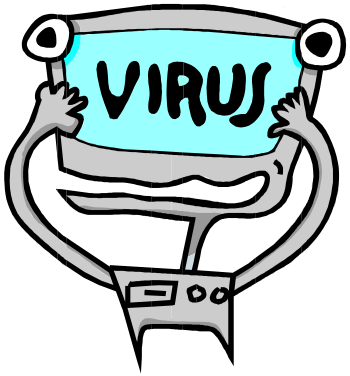
- Heute morgen am 12. Dezember 2006
  - 579.398 bekannte Viren
    - Ca. 80.000 Hauptstämme
    - Aktuell 2418 Viren „in the wild“



- 29.07.2006: 466.393 bekannte Viren
- 18.05.2006: 387.551 bekannte Viren
- 01.12.2005: 252.806 bekannte Viren

Virenanzahl bei verschiedenen Antiviren-Firmen

- Avira Antivir
  - 579.398 bekannte Viren und Schadprogramme
- Symantec
  - 73.011 Virenstämme
- ClamAV
  - 80.576 Virenstämme



Wer schreibt denn nun Viren und warum?

- Der „typische Virenprogrammierer“
  - Unter 25 Jahren
  - Männlich
  - „keine Freunde“ – sucht Anerkennung im Cyberspace
  - Nutzt Phantasienamen aus Fantasyromanen
  - Es gibt auch IT-Spezialisten, die Viren programmieren
- Kann auch ich einen Virus schreiben?
- Ist das strafbar?

Viren, Würmer und Trojaner

Tagesschau 2004-05-10

"Sasser"- Programmierer gefasst

Werbung im Internet nimmt zu

Ein Schüler aus Niedersachsen ist als mutmaßlicher Programmierer des Computerwurms "Sasser" festgenommen worden. Das Virus hatte in den vergangenen Tagen weltweit PCs lahm gelegt und Millionen-Schäden verursacht. Der 18-Jährige, der bei seinen Eltern in der Nähe der Stadt Rotenburg lebt, habe ein Geständnis abgelegt, sagte ein Sprecher der niedersächsischen Polizei. Auch Experten der Software-Firma Microsoft hätten inzwischen bestätigt, dass der junge Mann der Urheber des Computer-Wurms ist.

Nach Angaben der Polizei wurden alle Computer des Schülers beschlagnahmt. Es gebe keine Hinweise, dass er Kontakte zur organisierten Kriminalität habe, hieß es. Gegen den Jugendlichen werde nun wegen Computer-Sabotage ermittelt. Darauf stehen Strafen bis zu fünf Jahren Haft.

Schüler könnte auch "Netsky.ac" programmiert haben

Der 18-Jährige wird zudem verdächtigt, auch für das Virus "Netsky.ac" verantwortlich zu sein, das in der Nacht zum vergangenen Dienstag auftauchte. Microsoft will den Informanten, die dabei geholfen haben, den 18-Jährigen aufzuspüren, eine Belohnung von 250.000 Dollar zahlen. Das Geld solle aber erst nach seiner Verurteilung gezahlt werden, sagte der Microsoft-Vizepräsident Brad Smith. An der Suche

Wie kann sich mein Computer infizieren?

- Der Virus muss auf meinen PC gelangen
  - Speichermedien (z.B. CD, DVD, USB-Sticks)
  - Netzwerk (z.B. Internet)
- Der Viruscode muss ausgeführt werden
  - Programm starten
  - eMail und/oder Anhang öffnen
  - Webseite öffnen

Wie funktionieren Viren?

- Viren sind Computerprogramme
  - Grundsätzlich sind alle Systeme gefährdet, die in irgendeiner Form Programmcode ausführen können
- Viren können alles, was Programme auch können
  - Kopieren
  - Löschen
  - Verändern

Viren, Würmer und Trojaner

Welche Arten von Viren gibt es?

- Bootsektorviren (Parity Boot)
- Programmviren, Dateiviren (W32/Ska-Happy99)
- Makroviren (WM97/Melissa)
- Trojanische Pferde, Trojaner (Back Orifice 2000)
- Würmer (W32/Blaster, CodeRed, Sober.X)
- Script-Viren (VBS/LoveLet-A)
- Proof-of-Concept-Viren (W32/Sharp-A)
- Testviren (EICAR)
- Jokes (Joke/Buttons)
- Hoaxes (Good Times)
- Kettenbriefe (Bill Gates)

- Phishing

Nicht alle Viren sind gleich „erfolgreich“!

Viren, Würmer und Trojaner

Können Viren Schäden anrichten? Sind Viren wirklich ein Problem?

- Daten verändern (XM/Compatable)
- Daten löschen (Michelangelo)
- Daten ausspionieren (Loveletter)
- Fremdzugriff ermöglichen (Back Orifice 2000)
- Arbeit unmöglich machen (NightShade / Blaster)
- Computer zerstören (Chernobyl)

- Direkte Kosten (Telefonkosten 0190, Reparatur, Arbeitszeit, Bankkonto)
- Geschäftsschädigung
- Rufschädigung (Rassistische eMails)

Viren, Würmer und Trojaner

Beispiel: MyDoom-Varianten

FAZ 2004-01-31

Microsoft setzt 250 000 Dollar auf "Mydoom"-Urheber aus

Kaspersky: Programmierer stammt wohl aus Rußland / Bisher rund 2,6 Milliarden Dollar Schaden

mwe./ht. MOSKAU/FRANKFURT, 30. Januar. Der Softwarekonzern Microsoft hat 250 000 Dollar Kopfgeld auf den Programmierer des E-Mail-Wurms "Mydoom" ...

FAZ 2004-07-27

Computer-Viren

Neue "MyDoom"-Version lähmt Suchmaschinen

Ein Computerwurm hat am Montag zeitweilig die Funktionen bekannter Internet-Suchmaschinenen beeinträchtigt. Der Wurm - ein Nachfolger des berüchtigten ...

FAZ 2004-07-28

Internet-Wurm Mydoom legte Suchmaschine Google lahm

Virenschreiber ließ nach neuen E-Mail-Adressen suchen / Ausbreitung gestoppt

ht. FRANKFURT, 27. Juli. Die neueste Variante des Internet-Wurms Mydoom hat in den vergangenen Tagen nicht nur E-Mail-Postfächer überflutet, ...

Tagesschau 2004-07-27

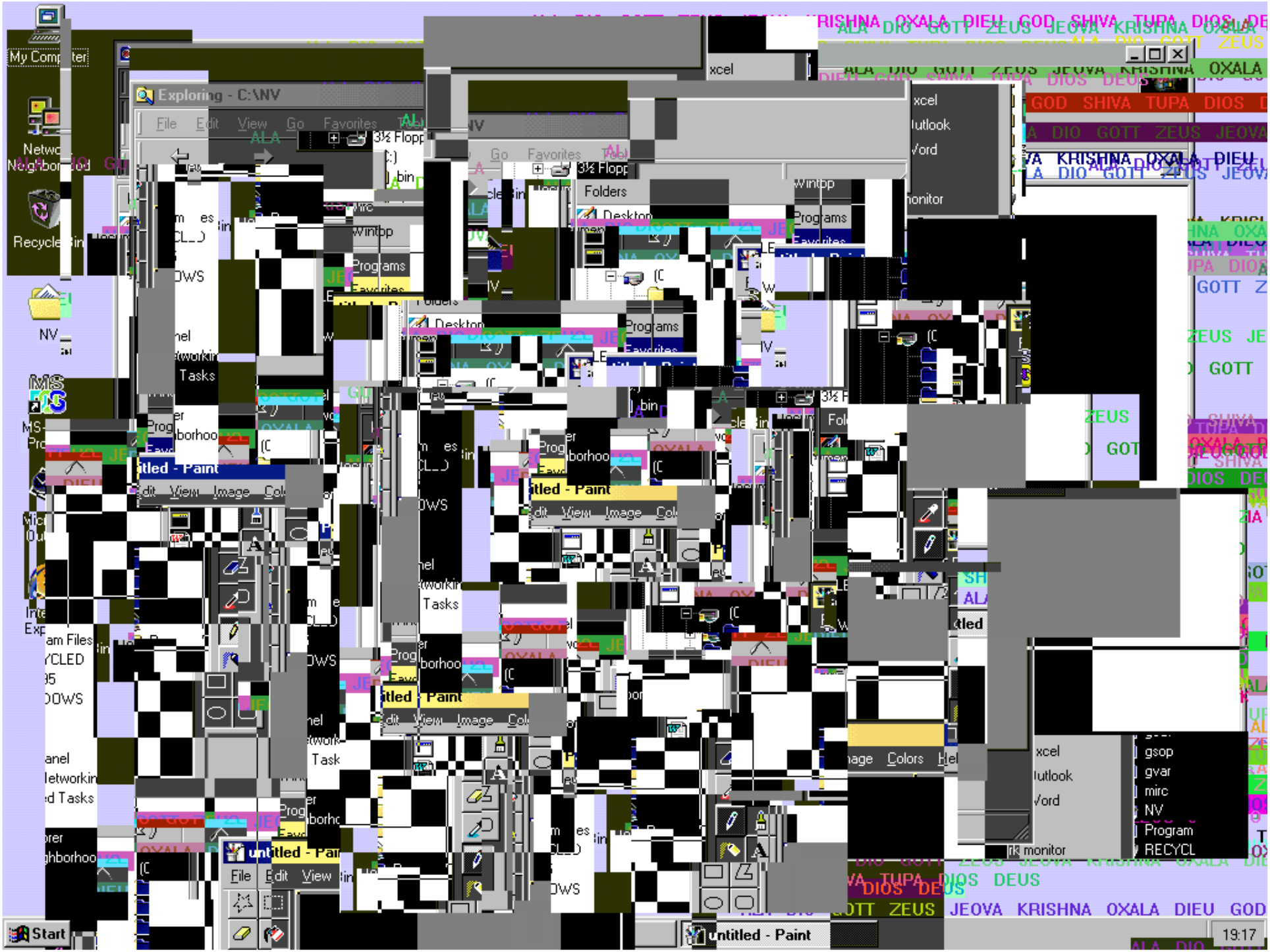
Neue MyDoom-Version

Internetwurm stört Suchmaschinen

Ein so genannter Internetwurm hat Experten zufolge die Funktion von Internet-Suchmaschinenen beeinträchtigt. Der Wurm sei anscheinend auch für den zweitweiligen Ausfall der Suchmaschine Google in den USA und einigen Ländern Europas verantwortlich. "Die jüngste Version von MyDoom, die verstärkt auf Mailboxen eingelaufen ist, benutzt die Suchmaschinen, um sich weiter zu verbreiten", teilte der US-Sicherheitsforschungsdienst SANS mit. Einige Suchmaschinen-Betreiber hätten sich über eine Beeinträchtigung der Leistung ihrer Großrechner beklagt.

Der Wurm MyDoom hatte Anfang Februar bereits weltweit für Aufregung gesorgt, als er unter anderem die Web-Seiten der US-Softwarefirma SCO lahm gelegt hatte. Experten hatten am Montag eine deutliche Verlangsamung der Performance bei verschiedenen Internet-Seiten festgestellt, als deren Ursache sie Viren-Attacken oder anders geartete Angriffe auf das Internet nicht ausgeschlossen hatten.


Setup for Microsoft Internet Explorer 3.01
Inbox
Recycle Bin
My Briefcase
Set Up The Microsoft Network
Start
En
1:15 AM


Exploring - C:\NV
untitled - Paint
Start
19:17

Viren, Würmer und Trojaner

Beispiel: Rufschädigung durch Sober

Tagesschau 2004-06-11

Online-Kriminalität

Computerkriminalität: Wurm verbreitet Hetz-Mails

Von Werbemails verstopfte E-Mail-Postfächer sind inzwischen traurige Realität. Immer häufiger kommen in den letzten Monaten dazu auch massenweise Mails, die von so genannten Würmern ohne das Wissen der Computerbesitzer verschickt werden. Wer diese Mails oder darin enthaltene Anhänge öffnet, fängt sich den Wurm in der Regel ebenfalls ein und wird so zur unfreiwilligen Versendestation.

Ausländerfeindliche Botschaften

Genau dieses Prinzip haben sich jetzt die Urheber eines Wurms zunutze gemacht, um rechtsradikale Hetz-Mails zu verbreiten. Sie griffen dabei auf einen bereits bekannten Schädling zurück: Sober. Die Mails enthalten Verweise zu rechtsradikalen Webseiten sowie ausländerfeindliche und rassistische Texte, die oft wie Nachrichten oder auch Leserbriefe formuliert sind.

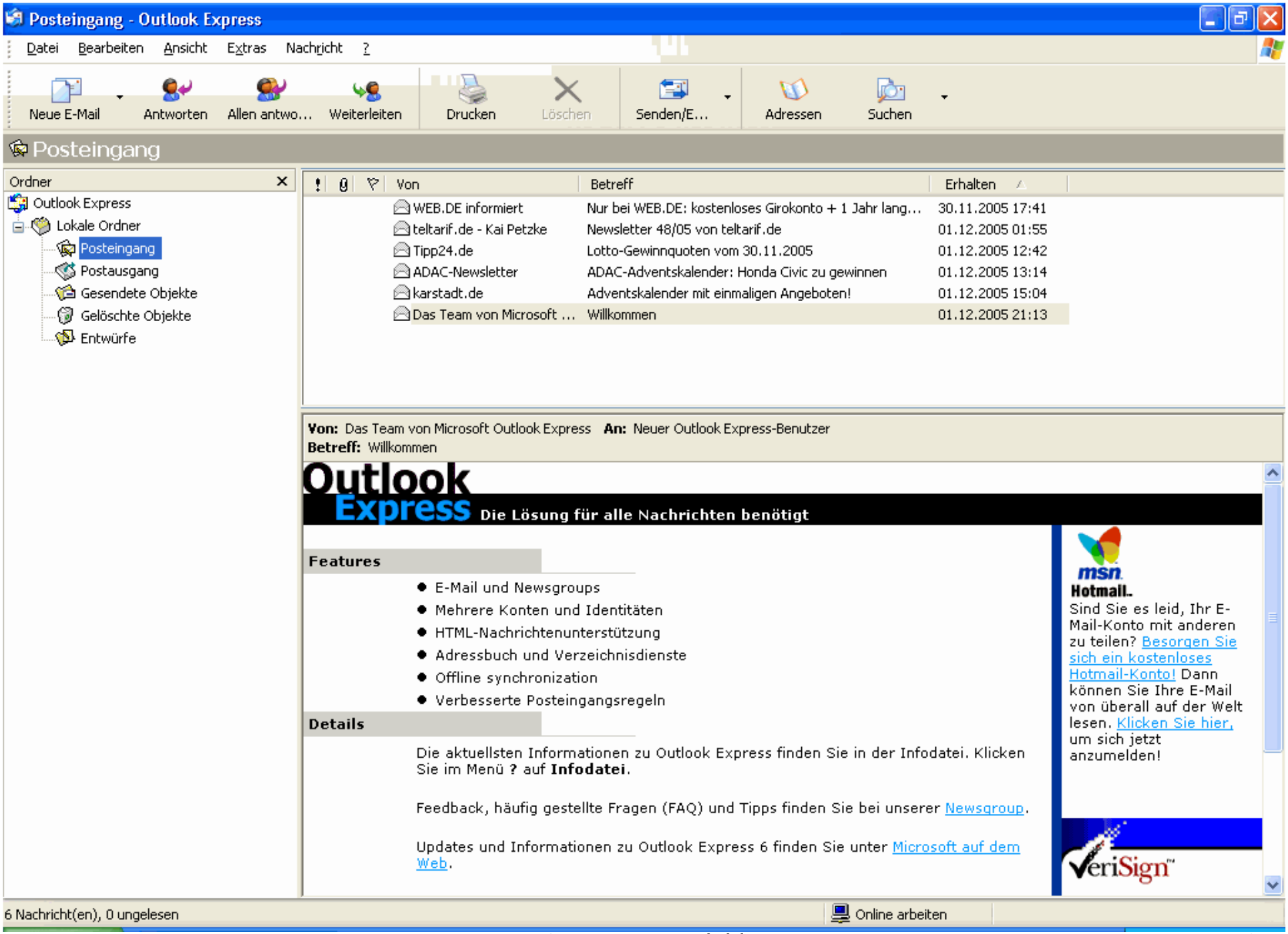
Die Betreffzeilen haben meist klar ausländerfeindliche Bezüge. Einige Beispiele: "Bankrott des Gesundheitswesens durch Auslaender!", "Auslaender erschleichen sich zunehmend Sozialleistungen", "MULTI-KULTI-BANDE TYRANNISIERTE MITSCHUELER" oder "ASYLANTEN BEGRABSCHTEN DEUTSCHES MAEDCHEN".

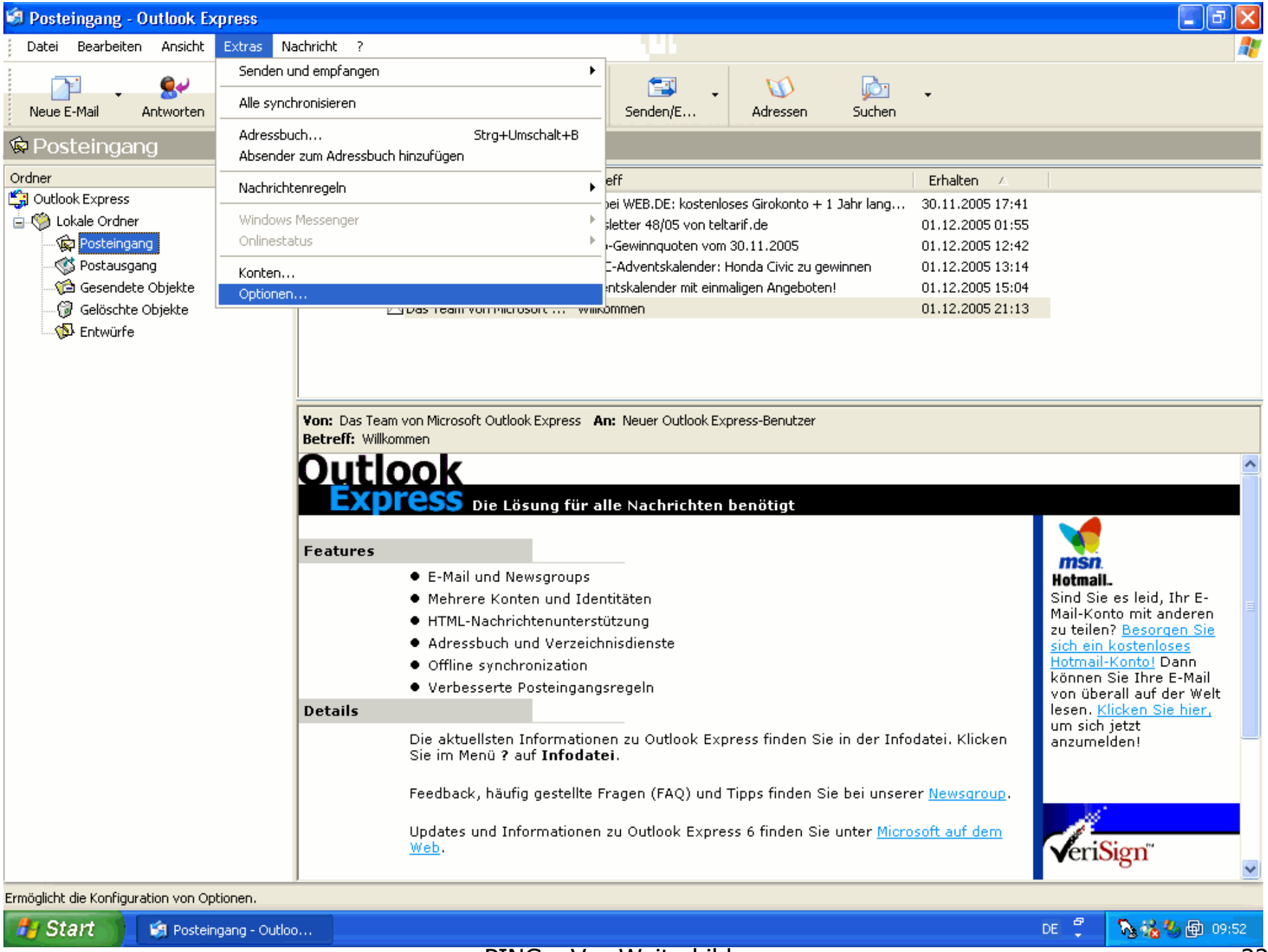
Ahnungslos werden Computerbesitzer zum Versender rechter Hetz-Mails.

Viren, Würmer und Trojaner

Wie kann ich mich schützen?

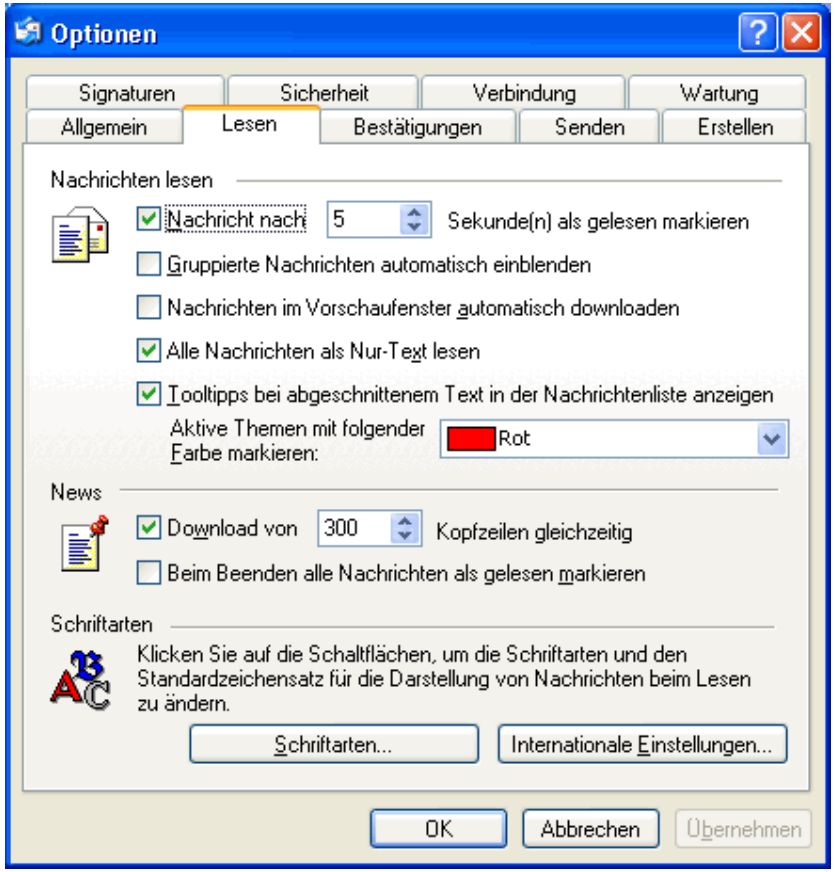
- Informiert sein (Weiterbildung)
- Keine fremden Datenträger nutzen
- Sicherheitseinstellungen (Browser) auf höchster Stufe
- Aktuelle Sicherheitsupdates installieren
- Einen Virenscanner installieren
- Immer die aktuelle Signaturen für den Virenscanner haben
- Personal Firewall installieren, bzw. eingebaute Firewall nutzen
- Weniger anfällige E-Mail-Clients und Browser verwenden
- E-Mail-Clients „sicher" konfigurieren
- Mails von unbekannten Absendern löschen
- Keine E-Mail-Anhänge ausführen
- Gesundes Misstrauen haben

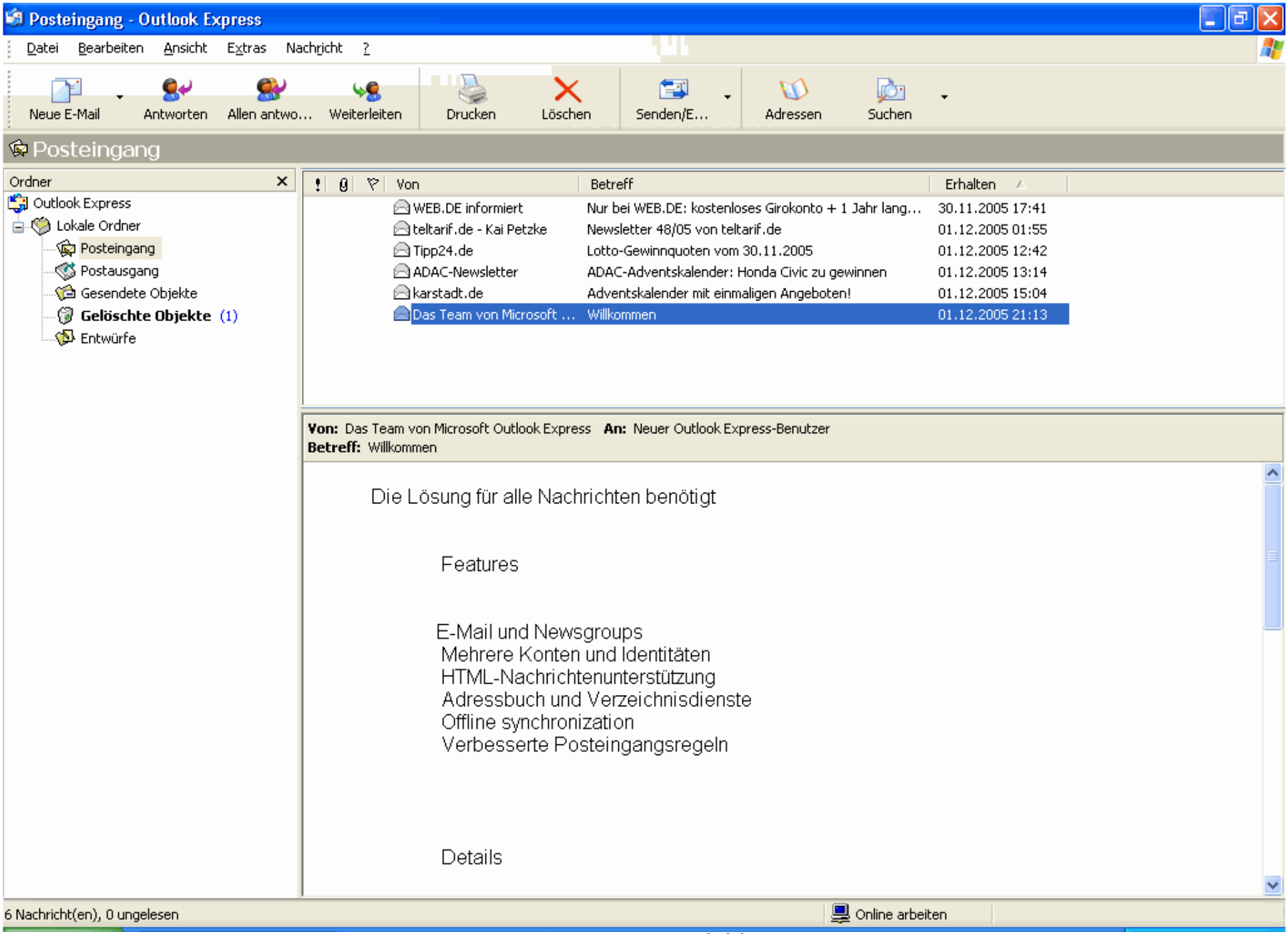

Posteingang - Outlook Express
Datei Bearbeiten Ansicht Extras Nachricht ?
Neue E-Mail
Antworten
Allen antwo...
Weiterleiten
Drucken
Löschen
Senden/E...
Adressen
Suchen
Posteingang
Ordner
Outlook Express
Lokale Ordner
Posteingang
Postausgang
Gesendete Objekte
Gelöschte Objekte
Entwürfe
Von
Betreff
Erhalten
WEB.DE informiert
Nur bei WEB.DE: kostenloses Girokonto + 1 Jahr lang...
30.11.2005 17:41
teltarif.de - Kai Petzke
Newsletter 48/05 von teltarif.de
01.12.2005 01:55
Tipp24.de
Lotto-Gewinnquoten vom 30.11.2005
01.12.2005 12:42
ADAC-Newsletter
ADAC-Adventskalender: Honda Civic zu gewinnen
01.12.2005 13:14
karstadt.de
Adventskalender mit einmaligen Angeboten!
01.12.2005 15:04
Das Team von Microsoft ...
Willkommen
01.12.2005 21:13
Von: Das Team von Microsoft Outlook Express An: Neuer Outlook Express-Benutzer
Betreff: Willkommen
Outlook Express
Die Lösung für alle Nachrichten benötigt
Features
E-Mail und Newsgroups
Mehrere Konten und Identitäten
HTML-Nachrichtenunterstützung
Adressbuch und Verzeichnisdienste
Offline synchronization
Verbesserte Posteingangsregeln
Details
Die aktuellsten Informationen zu Outlook Express finden Sie in der Infodatei. Klicken Sie im Menü ? auf Infodatei.
Feedback, häufig gestellte Fragen (FAQ) und Tipps finden Sie bei unserer Newsgroup.
Updates und Informationen zu Outlook Express 6 finden Sie unter Microsoft auf dem Web.
msn
Hotmail.
Sind Sie es leid, Ihr E-Mail-Konto mit anderen zu teilen? Besorgen Sie sich ein kostenloses Hotmail-Konto! Dann können Sie Ihre E-Mail von überall auf der Welt lesen. Klicken Sie hier, um sich jetzt anzumelden!
VeriSign
6 Nachricht(en), 0 ungelesen
Online arbeiten


Posteingang - Outlook Express
Datei Bearbeiten Ansicht Extras Nachricht ?
Senden und empfangen
Alle synchronisieren
Adressbuch... Strg+Umschalt+B
Absender zum Adressbuch hinzufügen
Nachrichtenregeln
Windows Messenger
Onlinestatus
Konten...
Optionen...
Neue E-Mail
Antworten
Senden/E...
Adressen
Suchen
Posteingang
Ordner
Outlook Express
Lokale Ordner
Posteingang
Postausgang
Gesendete Objekte
Gelöschte Objekte
Entwürfe
Erhalten
30.11.2005 17:41
01.12.2005 01:55
01.12.2005 12:42
01.12.2005 13:14
01.12.2005 15:04
01.12.2005 21:13
Von: Das Team von Microsoft Outlook Express An: Neuer Outlook Express-Benutzer
Betreff: Willkommen
Outlook Express
Die Lösung für alle Nachrichten benötigt
Features
E-Mail und Newsgroups
Mehrere Konten und Identitäten
HTML-Nachrichtenunterstützung
Adressbuch und Verzeichnisdienste
Offline synchronization
Verbesserte Posteingangsregeln
Details
Die aktuellsten Informationen zu Outlook Express finden Sie in der Infodatei. Klicken Sie im Menü ? auf Infodatei.
Feedback, häufig gestellte Fragen (FAQ) und Tipps finden Sie bei unserer Newsgroup.
Updates und Informationen zu Outlook Express 6 finden Sie unter Microsoft auf dem Web.
msn Hotmail.
Sind Sie es leid, Ihr E-Mail-Konto mit anderen zu teilen? Besorgen Sie sich ein kostenloses Hotmail-Konto! Dann können Sie Ihre E-Mail von überall auf der Welt lesen. Klicken Sie hier, um sich jetzt anzumelden!
VeriSign
Ermöglicht die Konfiguration von Optionen.
Start
Posteingang - Outloo...
DE
09:52

Viren, Würmer und Trojaner

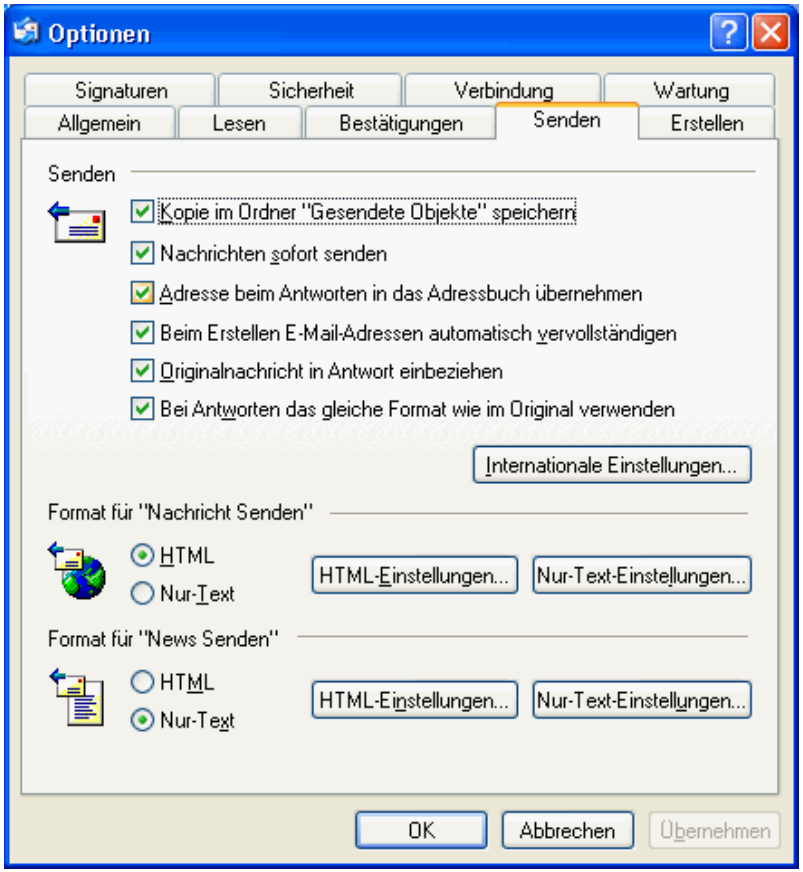
Wie schütze ich mich?
– Einstellungen für Outlook Express

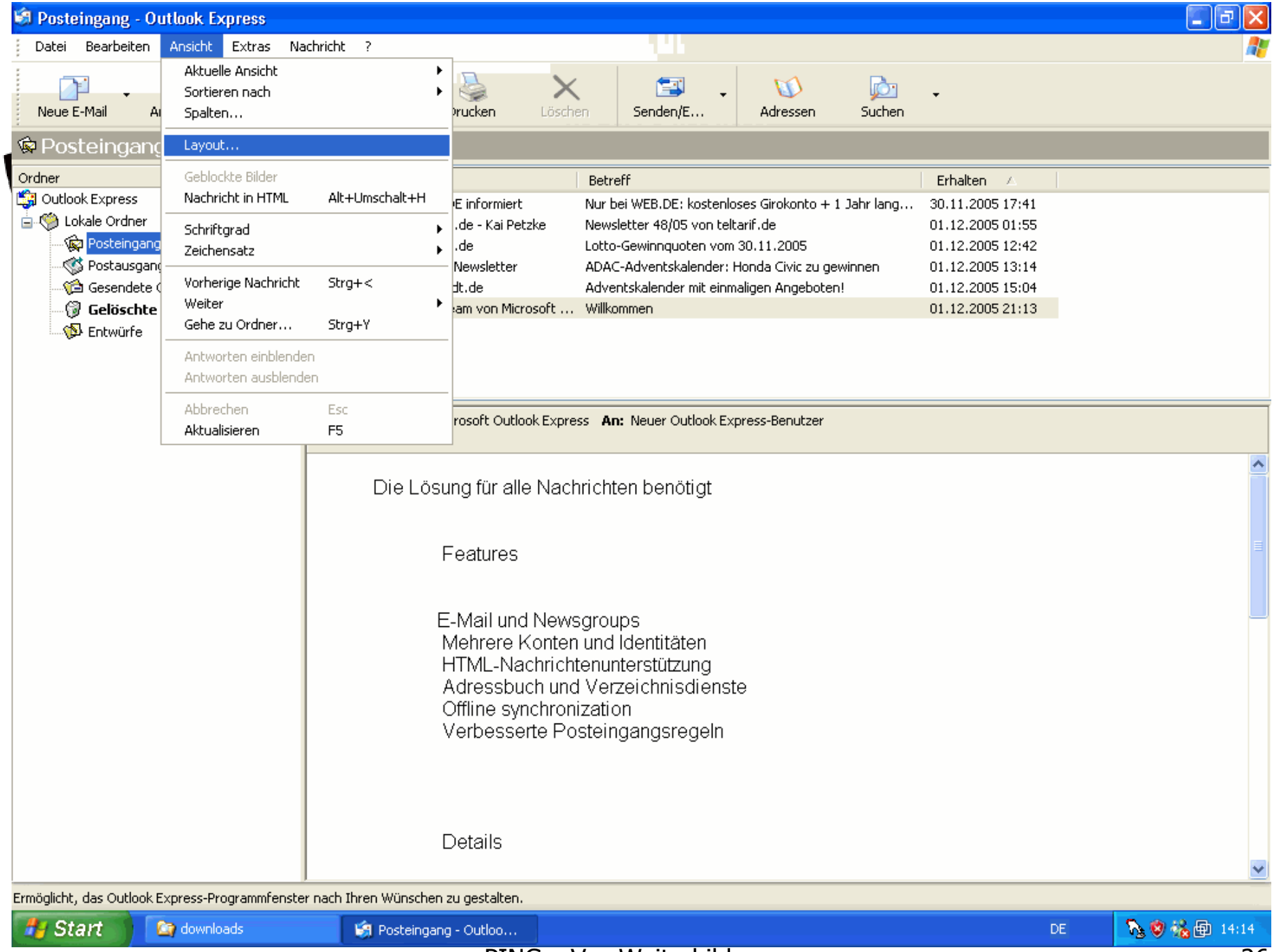



Posteingang - Outlook Express
Datei Bearbeiten Ansicht Extras Nachricht ?
Neue E-Mail
Antworten
Allen antwo...
Weiterleiten
Drucken
Löschen
Senden/E...
Adressen
Suchen
Posteingang
Ordner
Outlook Express
Lokale Ordner
Posteingang
Postausgang
Gesendete Objekte
Gelöschte Objekte (1)
Entwürfe
Von
Betreff
Erhalten
WEB.DE informiert
Nur bei WEB.DE: kostenloses Girokonto + 1 Jahr lang...
30.11.2005 17:41
teltarif.de - Kai Petzke
Newsletter 48/05 von teltarif.de
01.12.2005 01:55
Tipp24.de
Lotto-Gewinnquoten vom 30.11.2005
01.12.2005 12:42
ADAC-Newsletter
ADAC-Adventskalender: Honda Civic zu gewinnen
01.12.2005 13:14
karstadt.de
Adventskalender mit einmaligen Angeboten!
01.12.2005 15:04
Das Team von Microsoft ...
Willkommen
01.12.2005 21:13
Von: Das Team von Microsoft Outlook Express An: Neuer Outlook Express-Benutzer
Betreff: Willkommen
Die Lösung für alle Nachrichten benötigt
Features
E-Mail und Newsgroups
Mehrere Konten und Identitäten
HTML-Nachrichtenunterstützung
Adressbuch und Verzeichnisdienste
Offline synchronization
Verbesserte Posteingangsregeln
Details
6 Nachricht(en), 0 ungelesen
Online arbeiten

Viren, Würmer und Trojaner

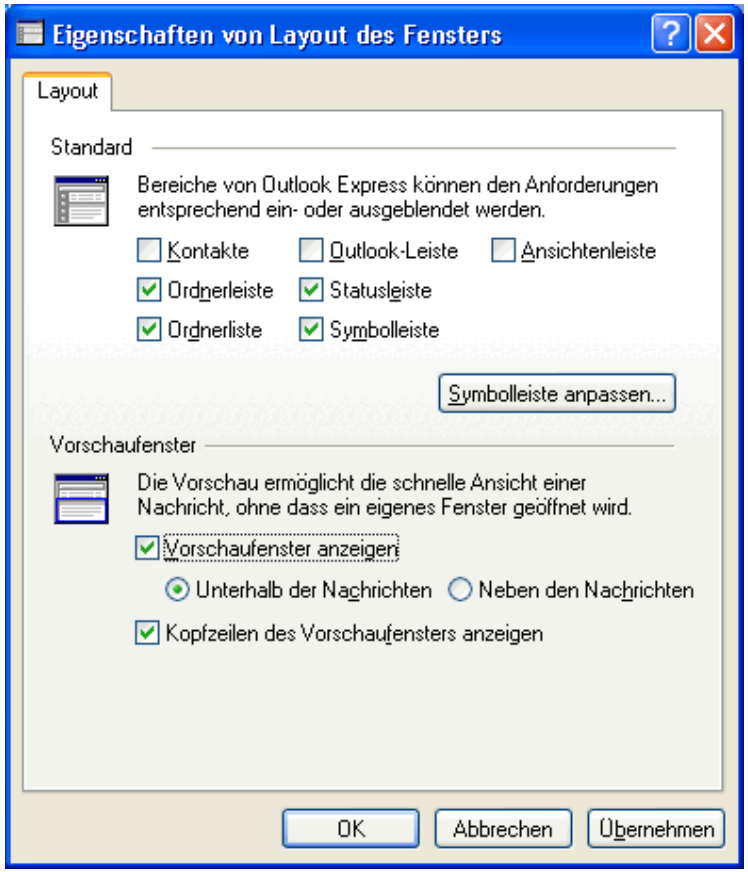
Wie schütze ich mich?
– Einstellungen für Outlook Express

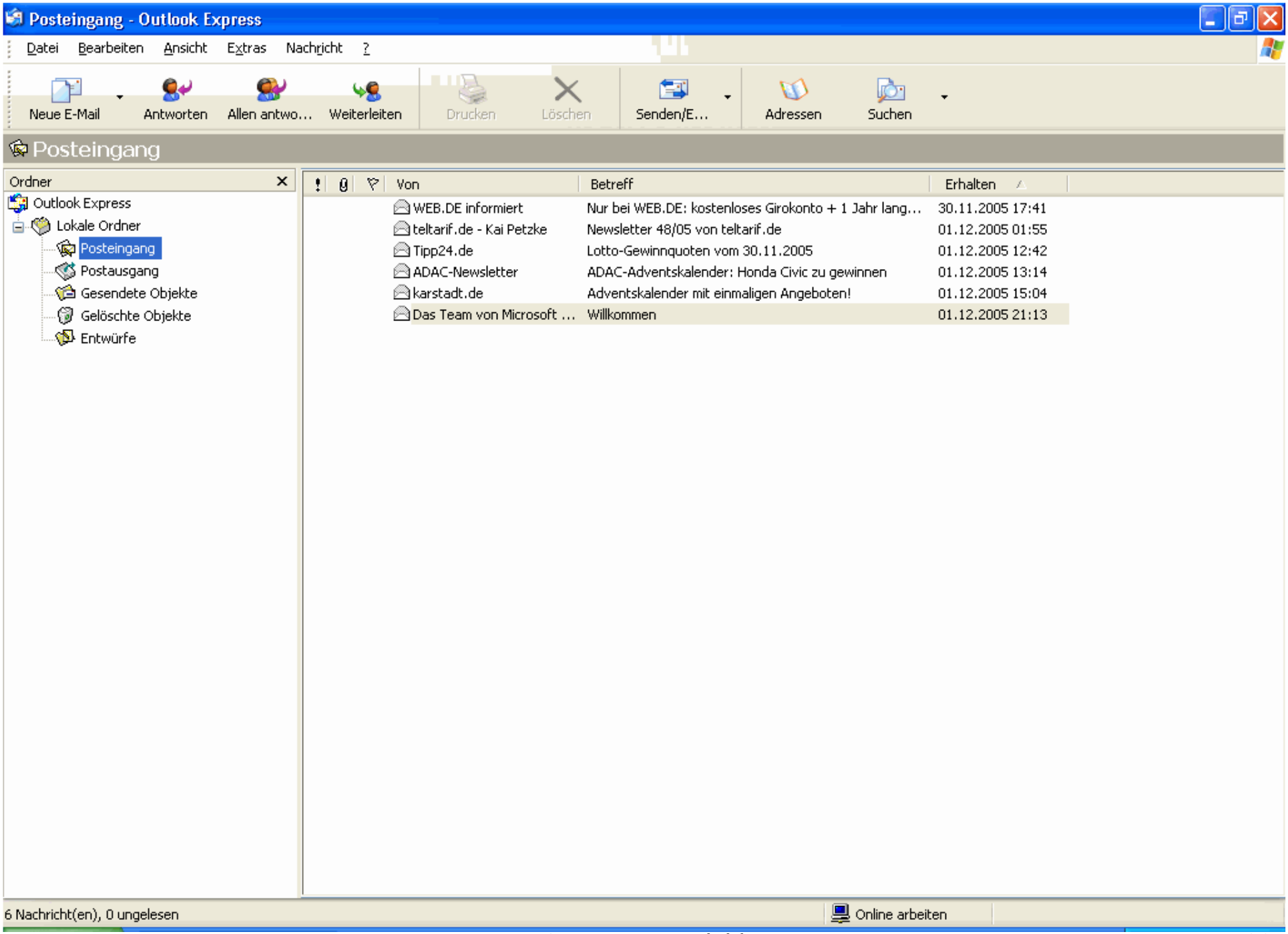



Posteingang - Outlook Express
Datei Bearbeiten Ansicht Extras Nachricht ?
Aktuelle Ansicht
Sortieren nach
Spalten...
Layout...
Geblockte Bilder
Nachricht in HTML Alt+Umschalt+H
Schriftgrad
Zeichensatz
Vorherige Nachricht Strg+<
Weiter
Gehe zu Ordner... Strg+Y
Antworten einblenden
Antworten ausblenden
Abbrechen Esc
Aktualisieren F5
Neue E-Mail
Senden/E...
Adressen
Suchen
Ordner
Outlook Express
Lokale Ordner
Posteingang
Gelöschte
Entwürfe
Betreff
Erhalten
Nur bei WEB.DE: kostenloses Girokonto + 1 Jahr lang... 30.11.2005 17:41
Newsletter 48/05 von teltarif.de 01.12.2005 01:55
Lotto-Gewinnquoten vom 30.11.2005 01:42
ADAC-Adventskalender: Honda Civic zu gewinnen 01.12.2005 13:14
Adventskalender mit einmaligen Angeboten! 01.12.2005 15:04
Willkommen 01.12.2005 21:13
An: Neuer Outlook Express-Benutzer
Die Lösung für alle Nachrichten benötigt
Features
E-Mail und Newsgroups
Mehrere Konten und Identitäten
HTML-Nachrichtenunterstützung
Adressbuch und Verzeichnisdienste
Offline synchronization
Verbesserte Posteingangsregeln
Details
Ermöglicht, das Outlook Express-Programmfenster nach Ihren Wünschen zu gestalten.
Start
downloads
Posteingang - Outloo...
DE
14:14

Viren, Würmer und Trojaner

Wie schütze ich mich?
- Einstellungen für Outlook Express




Posteingang - Outlook Express
Datei Bearbeiten Ansicht Extras Nachricht ?
Neue E-Mail
Antworten
Allen antwo...
Weiterleiten
Drucken
Löschen
Senden/E...
Adressen
Suchen
Posteingang
Ordner
Outlook Express
Lokale Ordner
Posteingang
Postausgang
Gesendete Objekte
Gelöschte Objekte
Entwürfe
Von
Betreff
Erhalten
WEB.DE informiert
Nur bei WEB.DE: kostenloses Girokonto + 1 Jahr lang...
30.11.2005 17:41
teltarif.de - Kai Petzke
Newsletter 48/05 von teltarif.de
01.12.2005 01:55
Tipp24.de
Lotto-Gewinnquoten vom 30.11.2005
01.12.2005 12:42
ADAC-Newsletter
ADAC-Adventskalender: Honda Civic zu gewinnen
01.12.2005 13:14
karstadt.de
Adventskalender mit einmaligen Angeboten!
01.12.2005 15:04
Das Team von Microsoft ...
Willkommen
01.12.2005 21:13
6 Nachricht(en), 0 ungelesen
Online arbeiten

Wie funktioniert ein Virenscanner?

- Unterschied „on access“ und „on demand“
- Prüfsummen (erkennt Veränderungen)
- Mustererkennung (erkennt bekannte Viren)
- Heuristische Methode (erkennt neue Viren)
- Simulation (erforscht neue Viren)

- Als Einzelplatz, lokale Installation
- Im Netzwerk
- Einbindung in Contentsecurity-Systeme
- In Verbindung mit Intrusion Detection Systemen

Was bringt die Zukunft?

- Viren in Transportmitteln (z.B. in Maut-Systemen, Navigations-Systemen)
- Viren in Haushaltsgeräten
- Cyberterrorismus (W32/Yaha-E / VBS/Staple-A)

Viren, Würmer und Trojaner

Was bringt die Zukunft?

- Viren bei Mobilfunk (Cabir-B)
- PDAs (Phage-963)

Viren durch mobiles Fernsehen?

Mittwoch 17. Mai 2006, 18:05 Uhr

von Elke Rekowski

(cid) - Handy-TV wird sich durchsetzen. Davon sind 100 Fach- und Führungskräfte überzeugt, die von der Beratungsgesellschaft Eurospace zum Thema "Mobilkommunikation" befragt wurden sind.

Mehr als ein Drittel der Manager (37 Prozent) geht davon aus, dass das "Taschenfernsehen" bereits in den nächsten zwei Jahren voll durchstarten wird. 26 Prozent der Befragten zeigten sich optimistisch: Handy-TV wird sich vor allem wegen der Fußball-WM bereits in diesem Jahr etablieren. An eine Durchdringung des Marktes mit dem Dienst in den nächsten fünf bis zehn Jahren glauben 16 Prozent der Führungskräfte, während zehn Prozent der Befragten der Ansicht sind, dass das Fernsehen im Mobiltelefon ein Flopp wird.

Viele der Manager (87 Prozent) zeigen sich jedoch auch ängstlich. Die Befürchtung: Im gleichem Maße, wie sich das Handy-TV etabliert, könnten Handy-Viren zu einem ernsthaften Problem werden. Die Mehrzahl (60 Prozent) der Befragten geht davon aus, dass diese Bedrohung im Jahr 2008 Realität werden wird. 17 Prozent der Führungskräfte vermuten sogar, dass es bereits in diesem Jahr Virenepidemien auf Handys geben könnte (www.eurospace.de).

- Pause -

Kontakt:

PING e.V.
Verein zur Förderung der privaten Internet Nutzung e.V.

Emil-Figge Str. 85
44227 Dortmund
Tel. 0231/9791 -0
FAX 0231/9791 -19
E-Mail: hotline@ping.de

Hotline-Zeiten:
Mittwochs 20-22 Uhr
Sonntags 19-21 Uhr

Weiterbildung:
www.ping.de/weiterbildung
weiterbildung@ping.de

„Viren, Würmer und Trojaner"

Daniel Borgmann
daniel@borgmann.ping.de

Dr. med. Arthur Pranada
ari@ping.de

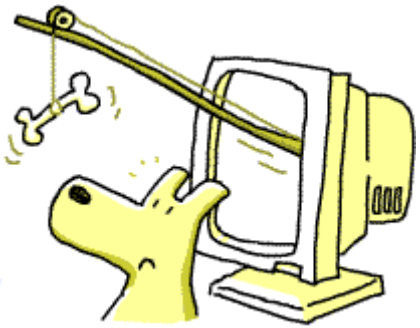
www.ping.de
Einfach mehr als nur Internet!

Nach der Pause:
- Vorsicht! – Betrüger und Abzocker im Internet: „Phishing"
- Praktische Beispiele

Vorsicht!
Abzocker und Betrüger im Internet …

Phishing

Phishing – „Passwort Fishing“



- Gefälschte E-Mails von Betrügern, die den Nutzer verleiten sollen, Zugangsdaten sowie andere geheime Informationen freiwillig preiszugeben
  - Online-Banking: Kontonummer, PIN, TAN
  - Kreditkartendaten
  - Zugangsdaten zu Online-Shops oder anderen kostenpflichtigen Diensten

Wie gehen die „Phisher“ vor?

- Nutzung fremder Rechner zum Versand der Mail
- Spiel mit der Angst und Unsicherheit der Anwender
  - „Sicherheitsüberprüfung“
  - Neues „Sicherheitssystem“
- Absender der E-Mails ist gefälscht
  - security@[bankname].com
- E-Mail beinhaltet Erkennungsmerkmale der Bank
  - Logo / Kontaktadressen
- Sicherheitslücken in Browser/Betriebssystem werden genutzt
- Anwender wird auf gefälschte Anmeldeseite gelockt, die der echten Seite täuschend ähnlich sieht
  - Beschriftung von Links in der E-Mail stimmt nicht mit der tatsächlichen Adresse überein
  - Oft handelt es sich um „gehackte Rechner“

Beispiele für Phishing

Wie Betrüger an Ihr Geld kommen wollen …

Wie schütze ich mich vor „Phishern“?

- Gesundes Misstrauen!
  - Keine Bank fragt unaufgefordert nach Ihren geheimen Zugangsdaten
  - Niemals die PIN/TAN an Fremde geben
  - Informieren Sie sich, welche Zugangsdaten normalerweise von der Bank abgefragt werden!
  - Fragen Sie bei ungewöhnlichen Aktivitäten lieber bei Ihrer Bank nach!
- Niemals Links in E-Mails anklicken!
  - Adressen immer von Hand eingeben oder eigene Bookmarks benutzen!
- Überprüfen Sie auf welcher Seite Sie sich befinden!
- Prüfen Sie die SSL-Zertifikate!
- Melden Sie ungewöhnliche Aktivitäten Ihrer Bank!
- Provider kann ggf. gefälschte Massen-E-Mails filtern
- Aktuelle Sicherheitsupdates einspielen!

„Phisher“ werde immer erfolgreicher

Wie Betrüger um Ihre Mithilfe bitten …

Viren, Würmer und Trojaner

Immer höhere Schäden durch Phishing und Identitätsdiebstahl...

news 02.04.2006 11:29

USA: Jährlich 6,4 Milliarden Schaden durch Identitätsdiebstahl

In den USA sei Privatpersonen 2004 ein geschätzter Schaden von 6,4 Milliarden US-Dollar durch Indentitätsdiebstahl entstanden. Das berichtet das US-amerikanische Justizministerium in seiner gerade veröffentlichten **jährlichen Kriminalstatistik[1]**. 3,6 Millionen beziehungsweise drei Prozent aller US-amerikanischen Haushalte haben demnach alleine im ersten Halbjahr 2004 finanziellen Schaden durch Identitätsklau erlitten.

Beinahe die Hälfte dieser Fälle ging der Statistik zufolge auf Missbrauch von Kreditkartendaten zurück. Bei 25 Prozent der Opfer habe das Erschleichen von Onlinebanking-Daten eine Rolle gespielt. Für seine Statistik befragte das Department of Justice alle sechs Monate rund 42.000 US-amerikanische Haushalte. In dem seit 30 Jahren erscheinenden Report wurde jetzt erstmalig Identitätsdiebstahl als eigenständige Delikt-Kategorie aufgenommen.

(**hob[2]**/c't) (hob/c't)

Viren, Würmer und Trojaner

Immer mehr Phishing-Opfer ...

news 14.03.2006 21:09

Phisher schwimmen in gestohlenen Geheimnummern

Nach Erkenntnissen der Arbeitsgruppe Identitätsschutz im Internet (**a-i3[1]**) suchen Phisher derzeit massiv nach Geldwäsche-Helfern, weil sie sich mit betrügerischen E-Mails mehr Geheimnummern "erarbeiten", als sie für Überweisungen von fremden Konten nutzen können. Kontoinhaber sollten keinesfalls Aufträge annehmen, die darin bestehen, Überweisungen anzunehmen und das Geld (meist abzüglich einer verlockenden Provision) weiterzuleiten.

Obacht gilt es daher nicht nur beim Umgang mit Kontoauszügen walten zu lassen, sondern etwa auch bei eBay-Verkäufen: Phisher können sich auf einfache Weise Bankdaten beschaffen, indem sie dort Waren ersteigern. Wenn beim Verkäufer eine extrem überhöhte Bezahlung eingeht, gefolgt von der Bitte, die "versehentliche" Überbezahlung per Western Union oder auf andere Weise in bar zurückzuzahlen, besteht dringender Geldwäsche-Verdacht.

In ihrem Vortrag auf dem **Heise-CeBIT-Forum [2]** berichteten Christoph Wegener und Dennis Werner

Geldwäsche-Mails

- Phisher „bitten“ inzwischen um Mithilfe, um an das erbeutete Geld zu kommen
  - Über das Internet (E-Mail) werden „Finanzagenten“ oder „Mitarbeiter/Vertriebspartner“ angeworben
  - Diese sollen das erphishte Geld ins Ausland transferieren
  - Achtung: Geldwäsche ist strafbar!
    (AG Darmstadt, Urteil vom 11.1.2006, Az. 212 Ls 360 Js 33848/05)

Geldwäsche ist strafbar!

news 19.04.2006 09:13

Phishing: Hohe Strafe gegen Finanzagenten

Das bundesweit zweite Urteil gegen einen so genannten Finanzagenten bei Phishing-Betrügereien liegt nun vor, teilte die "**Arbeitsgruppe Identitätsschutz im Internet[1]**" mit (AG Darmstadt, Urteil vom 11. 1. 2006, Az. 212 Ls 360 Js 33848/05 – **PDF-Datei[2]**).

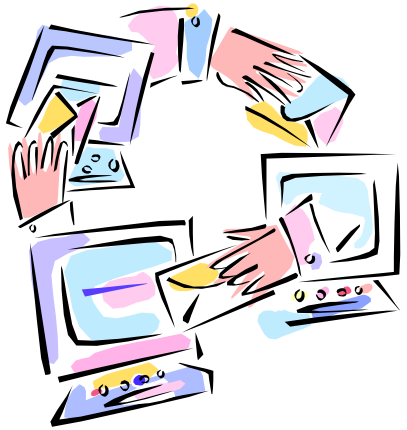
Phishing, das "Abfischen" vertraulicher Daten wie etwa Bankzugangsdaten, Kreditkartennummern, eBay-Accounts und Ähnlichem, hat sich längst von einer irrlichternen Randerscheinung des Online-Bankings zum handfesten wirtschaftlichen Problem entwickelt. Nun rücken auch verstärkt die für die

Informieren Sie sich…

- Arbeitsgruppe Identitätsschutz im Internet
  https://www.a-i3.org/
- Anti-Phishing Working Group
  http://www.antiphishing.org/
- Heise Security
  http://www.heise.de/security/
- Bundesamt für Sicherheit in der Informationstechnik
  http://www.bsi.de/
  http://www.bsi-fuer-buerger.de/

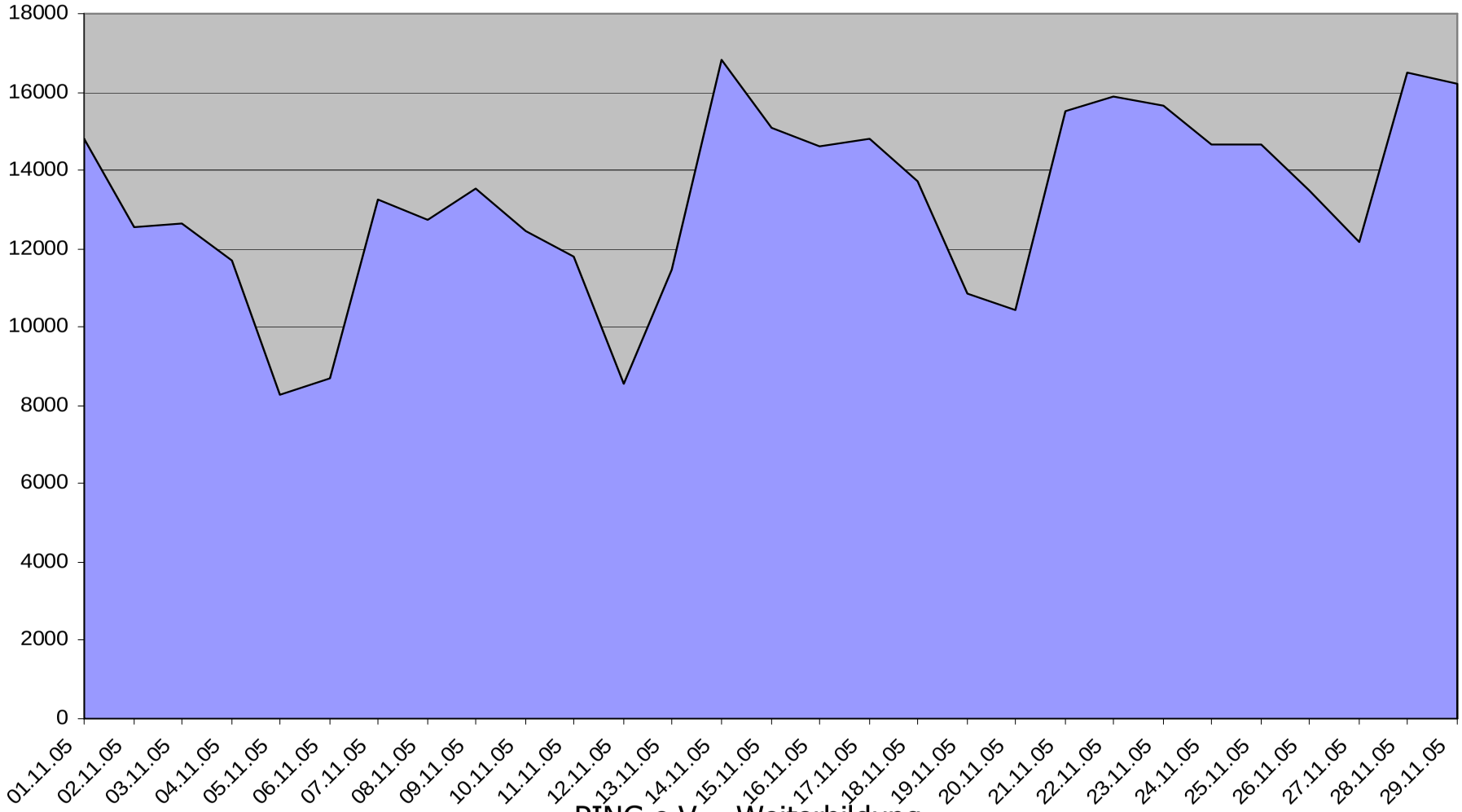
Wie können Internet-Provider helfen?

- Scanning-Systeme für E-Mails
  - Viren
  - Spam
  - Phishing
- Mehrstufige Firewalls
- Information der Mitglieder/Kunden
- Weiterbildungsveranstaltungen



Viren, Würmer und Trojaner

Mail-Aufkommen bei PING



Mail-Filtering bei PING – Dezember 2006

- Dezember 2006: Insgesamt 125084 Mails gefiltert
  - Davon 8757 Virenmails, davon
    - 7910 Phishing-Mails
    - 604 Viren/Würmer
    - 213 Trojaner
  - 107600 Spam-Mails
- November 2005: Insgesamt 31166 Mails gefiltert
  - Davon 2558 Virenmails
    - Davon 1125 Mails mit Sober.X/U
    - 1070 Phishing Mails
  - 28609 Spam-Mails

Vielen Dank für Ihre Aufmerksamkeit!

Für Fragen steht das PING-Team gerne zur Verfügung!

www.ping.de

Einfach mehr als nur Internet!

Viren, Würmer und Trojaner

Kontakt:

PING e.V.

Verein zur Förderung der privaten Internet Nutzung e.V.

Emil-Figge Str. 85
44227 Dortmund
Tel. 0231/9791 -0
FAX 0231/9791 -19
E-Mail: hotline@ping.de

Hotline-Zeiten:
Mittwochs 20-22 Uhr
Sonntags 19-21 Uhr

Weiterbildung:
www.ping.de/weiterbildung
weiterbildung@ping.de

„Viren, Würmer und Trojaner"

Daniel Borgmann
daniel@borgmann.ping.de

Dr. med. Arthur Pranada
ari@ping.de

www.ping.de

Einfach mehr als nur Internet!

Besuchen sie auch unsere übrigen kostenlosen Weiterbildungsveranstaltungen!

http://www.ping.de/weiterbildung/