"Achtung Virenalarm" – Perimeterschutz als Sicherheitslösung für Ihr Unternehmen

Erfahrungsaustausch

29.1.2004

Ing. Pumberger Christian

IG:IS Interessengemeinschaft Informationssicherheit

Zur Person

Ing. Pumberger Christian

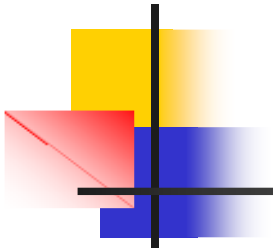
IT-Sicherheitsbeauftragter und Teamleiter IT-Infrastruktur bei der HYPO Tirol Bank AG

Alter: 34 Jahre

Seit 1991 mit dem Thema IT-Sicherheit beschäftigt.

Agenda

- Rückblick 2003
- Perimeterschutz
  - Gefahrenquellen
  - Genügt das alleine?
  - Lösungsansatz
- Ausblick 2004



IG:IS

Rückblick

2003

Rückblick 2003

Viren

Rang	Virus	Prozentualer Anteil
1	W32/Sobig-F	19.9%
2	W32/Blaster-A	15.1%
3	W32/Nachi-A	8.4%
4	W32/Gibe-F	7.2%
5	W32/Dumaru-A	6.1%
6	W32/Sober-A	5.8%
7	W32/Mimail-A	4.8%
8	W32/Bugbear-B	3.1%
9	W32/Sobig-E	2.9%
10	W32/Klez-H	1.6%
	Sonstige	25.1%

7.064 neue Viren, Würmer und Trojanische Pferde von insgesamt 86.000 Schadprogrammen.

Quelle: Sophos

Rückblick 2003

Acrobat Reader - [truesecure_Wildtrends.pdf]

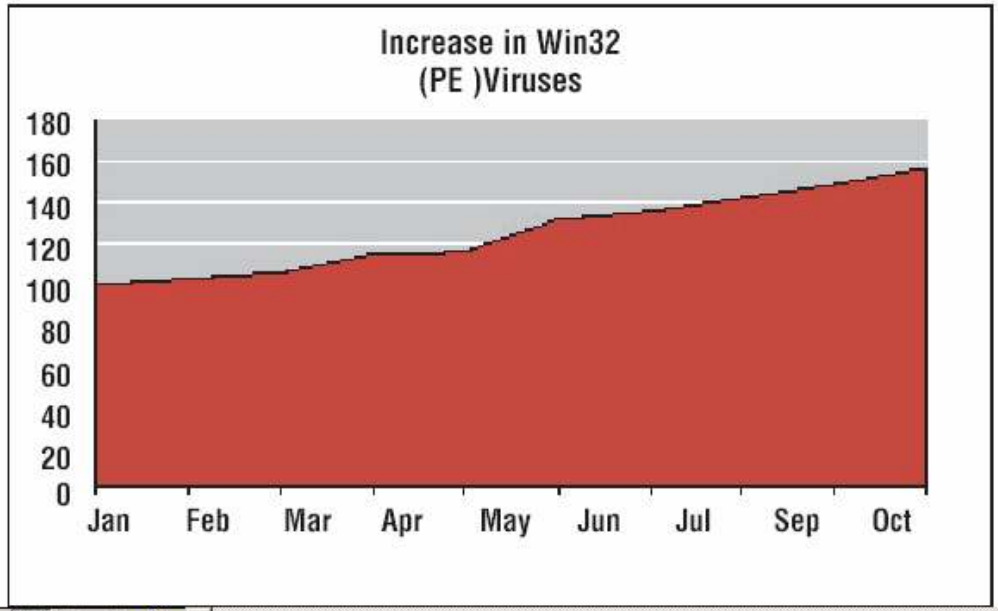
File Edit Document View Window Help

Bookmarks Thumbnails

Virus Type	Beginning of 2003	End of 2003	Change
Boot Sector Viruses	10	9	-10%
Script Viruses	16	14	-13%
Win32 (PE) Viruses	101	157	+55%
Win95 Viruses	11	12	+09%
Macro Viruses	67	63	-6%
TOTAL	205	255	+24%

Table 2: Increase or decrease in virus types

The greatest increase was with Win32 (PE) viruses as shown in Graph 2.



3 of 8 8,5 x 11 in

Quelle: Truesecure

Rückblick 2003

Virenscanner Aktualisierungszeiten

		Kaspersky	Trend Micro	Symantec	Sophos	McAfee	
Fizzer	08.05.2003	10.05.2003	12.05.2003	09.05.2003	09.05.2003	12.05.2003	4 Tage
Bugbear.b	4.6.2003-5.6.2003	05.06.2003 12:20	05.06.2003 09:40	05.06.2003 12:20	05.06.2003 12:30	05.06.2003 17:30	07:50 Stunde
Sober.C	20.12.2003 03:00	20.12.2003 14:45	20.12.2003 19:50	21.12.2003 04:05	21.12.2003 14:35	22.12.2003 04:10	2 Tage

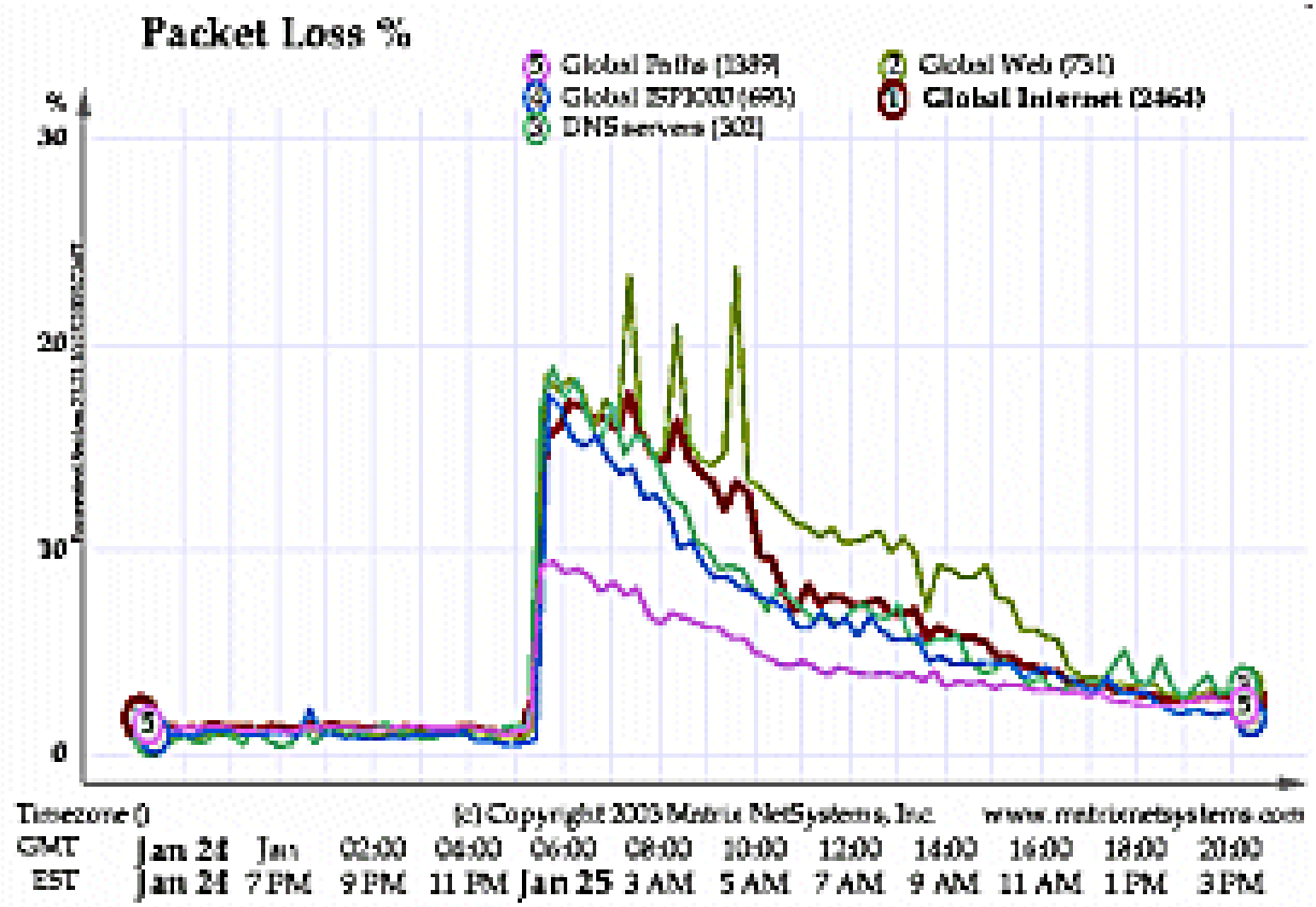
Dies stellt nur einen kleinen Ausschnitt der Produkte und der dokumentierten Zeiten dar.
Quelle: PC-Welt/www.av-test.org

Rückblick 2003

Slammer-Wurm

- In der Theorie gibt es 4 Milliarden öffentliche IP-Adressen im Internet.
- Der Slammer-Wurm wurde am 25.1.2003 um ca. 04:31 UTC freigesetzt.
- Um 04:45 wurden alle IP-Adressen gescannt – in weniger als 15 Minuten!!!!
- Folge war eine extreme Überlastung des Netzes.

Rückblick 2003



Rückblick 2003

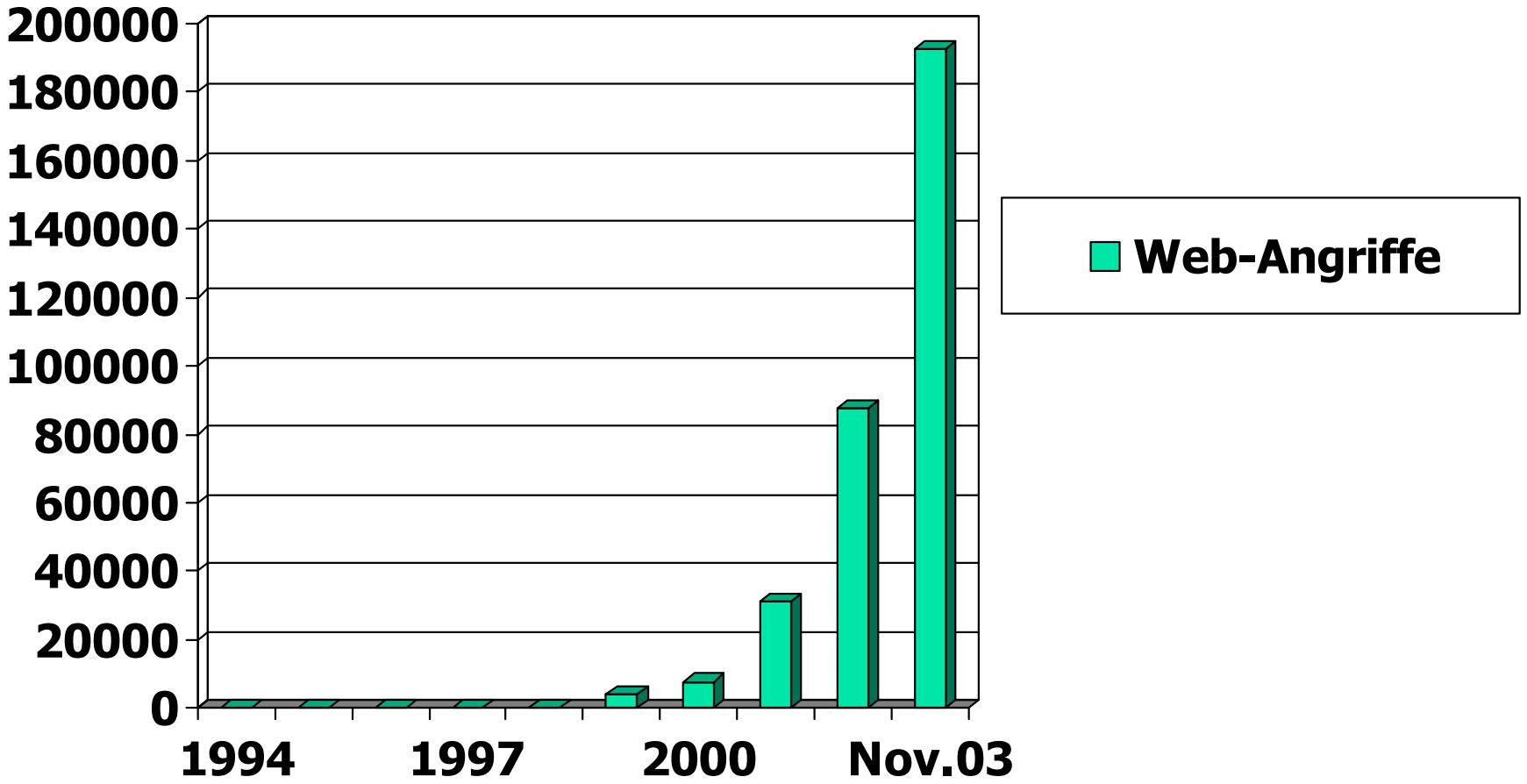
Alles nur Theorie? Wir sind nie betroffen?

- **Slammer:**
  - Internet war total überlastet
  - Eines der größten Bankomat-Netze ist abgestürzt und war über das gesamte Wochenende nicht erreichbar.
  - Viele int. Flughäfen meldeten, daß ihre Flugkontrollesystem Performance-Probleme hatten.
  - Im Davis-Besse Atomkraftwerk in Ohio wurde das Überwachungssystem des Reaktors lahmgelegt.
  - Notfallnummersysteme meldeten Probleme in einigen Regionen der USA
- **Blaster und Welchi**
  - Einige Flughäfen meldeten Probleme, die zur Stornierungen von Flügen führten.
  - Bankomaten der Fa. Diebold mit Windows-XP waren betroffen
  - Eisenbahn CSX hatte nach Problemen mit dem Zug-Leitsystem alle Pendlerzüge im Bereich US-Hauptstadt auf offener Streck angehalten.

Quelle: F-Secure

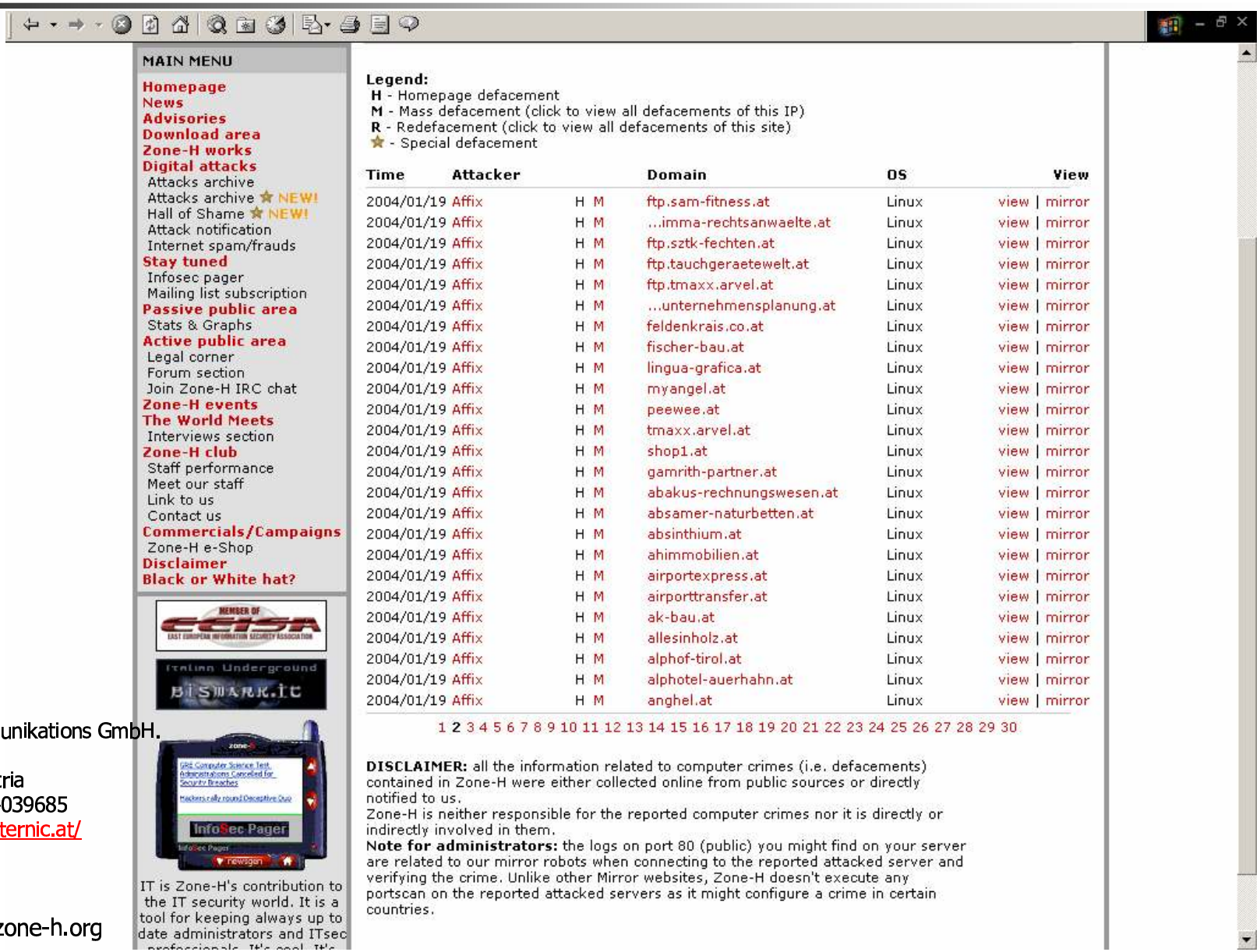
Rückblick 2003

Web-Angriffe



Quelle: www.mi2g.com

Rückblick 2003



MAIN MENU

- Homepage
- News
- Advisories
- Download area
- Zone-H works
- Digital attacks
  - Attacks archive
  - Attacks archive ★ NEW!
  - Hall of Shame ★ NEW!
  - Attack notification
  - Internet spam/frauds
- Stay tuned
  - Infosec pager
  - Mailing list subscription
- Passive public area
  - Stats & Graphs
- Active public area
  - Legal corner
  - Forum section
  - Join Zone-H IRC chat
- Zone-H events
- The World Meets
  - Interviews section
- Zone-H club
  - Staff performance
  - Meet our staff
  - Link to us
  - Contact us
- Commercials/Campaigns
  - Zone-H e-Shop
- Disclaimer
- Black or White hat?

IT is Zone-H's contribution to the IT security world. It is a tool for keeping always up to date administrators and ITsec

Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
★ - Special defacement

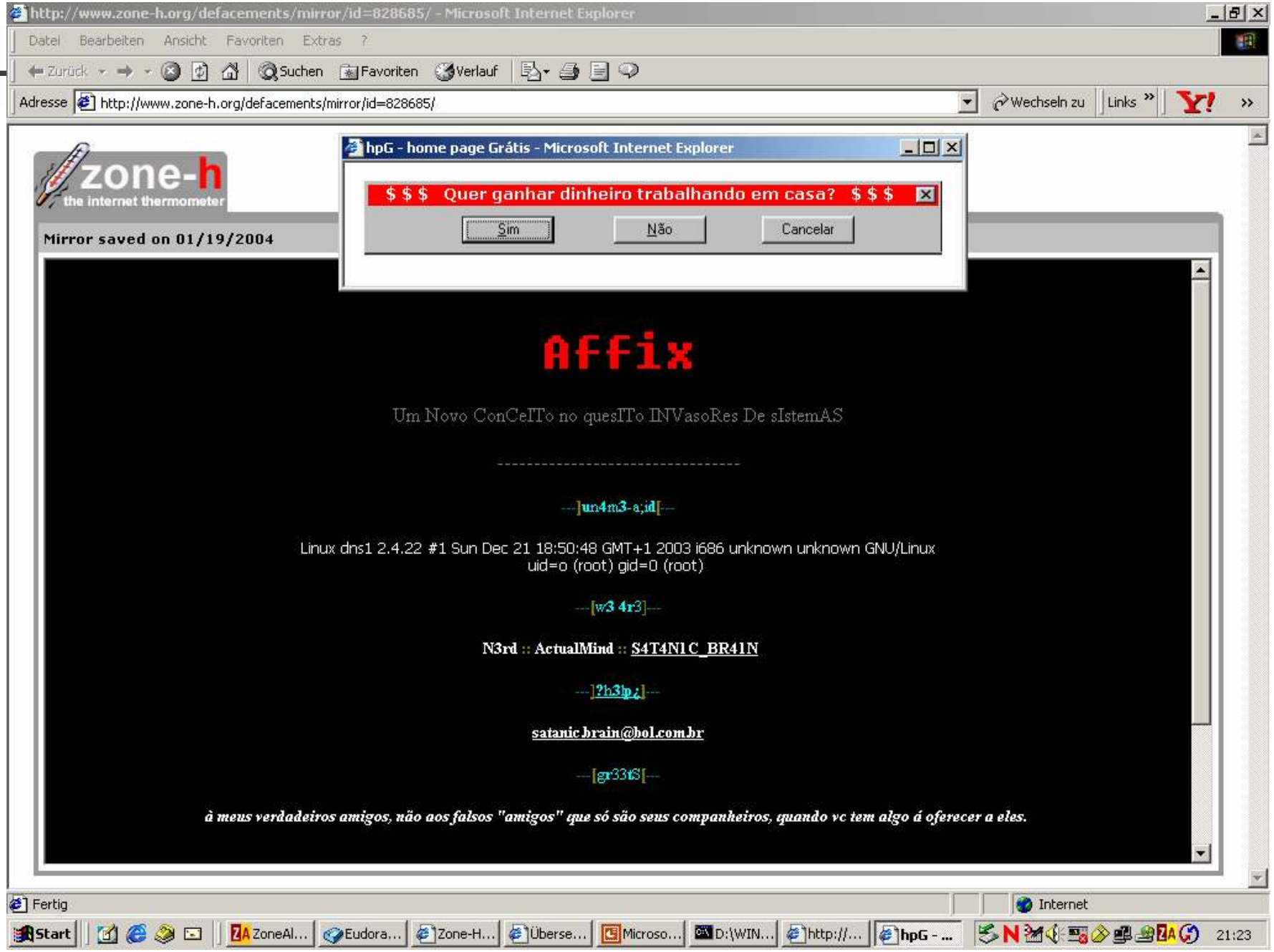
Time	Attacker			Domain	OS	View
2004/01/19	Affix	H	M	ftp.sam-fitness.at	Linux	view | mirror
2004/01/19	Affix	H	M	...imma-rechtsanwaelte.at	Linux	view | mirror
2004/01/19	Affix	H	M	ftp.sztk-fechten.at	Linux	view | mirror
2004/01/19	Affix	H	M	ftp.tauchgeraetewelt.at	Linux	view | mirror
2004/01/19	Affix	H	M	ftp.tmaxx.arvel.at	Linux	view | mirror
2004/01/19	Affix	H	M	...unternehmensplanung.at	Linux	view | mirror
2004/01/19	Affix	H	M	feldenkrais.co.at	Linux	view | mirror
2004/01/19	Affix	H	M	fischer-bau.at	Linux	view | mirror
2004/01/19	Affix	H	M	lingua-grafica.at	Linux	view | mirror
2004/01/19	Affix	H	M	myangel.at	Linux	view | mirror
2004/01/19	Affix	H	M	peewee.at	Linux	view | mirror
2004/01/19	Affix	H	M	tmaxx.arvel.at	Linux	view | mirror
2004/01/19	Affix	H	M	shop1.at	Linux	view | mirror
2004/01/19	Affix	H	M	gamrith-partner.at	Linux	view | mirror
2004/01/19	Affix	H	M	abakus-rechnungswesen.at	Linux	view | mirror
2004/01/19	Affix	H	M	absamer-naturbetten.at	Linux	view | mirror
2004/01/19	Affix	H	M	absinthium.at	Linux	view | mirror
2004/01/19	Affix	H	M	ahimmobilien.at	Linux	view | mirror
2004/01/19	Affix	H	M	airportexpress.at	Linux	view | mirror
2004/01/19	Affix	H	M	airporttransfer.at	Linux	view | mirror
2004/01/19	Affix	H	M	ak-bau.at	Linux	view | mirror
2004/01/19	Affix	H	M	allesinholz.at	Linux	view | mirror
2004/01/19	Affix	H	M	alphof-tirol.at	Linux	view | mirror
2004/01/19	Affix	H	M	alphotel-auerhahn.at	Linux	view | mirror
2004/01/19	Affix	H	M	anghel.at	Linux	view | mirror

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30

DISCLAIMER: all the information related to computer crimes (i.e. defacements) contained in Zone-H were either collected online from public sources or directly notified to us.
Zone-H is neither responsible for the reported computer crimes nor it is directly or indirectly involved in them.
Note for administrators: the logs on port 80 (public) you might find on your server are related to our mirror robots when connecting to the reported attacked server and verifying the crime. Unlike other Mirror websites, Zone-H doesn't execute any portscan on the reported attacked servers as it might configure a crime in certain countries.

212.126.66.20
internic Datenkommunikations GmbH.
Donaucitystr. 1
A-1220 Vienna, Austria
Telephone: +43(1)4039685
Web: http://www.internic.at/

Quelle: www.zone-h.org


http://www.zone-h.org/defacements/mirror/id=828685/ - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück Suchen Favoriten Verlauf
Adresse http://www.zone-h.org/defacements/mirror/id=828685/
Wechseln zu Links
zone-h
the internet thermometer
Mirror saved on 01/19/2004
hpG - home page Grátis - Microsoft Internet Explorer
$ $ $ Quer ganhar dinheiro trabalhando em casa? $ $ $
Sim
Não
Cancelar
Affix
Um Novo ConCeITo no quesITo INVasoRes De sIstemAS

---]un4m3-a;id[---
Linux dns1 2.4.22 #1 Sun Dec 21 18:50:48 GMT+1 2003 i686 unknown unknown GNU/Linux
uid=0 (root) gid=0 (root)
---[w3 4r3]---
N3rd :: ActualMind :: S4T4N1C_BR41N
---]?h3lp¿]---
satanic.brain@bol.com.br
---[gr33tS[---
à meus verdadeiros amigos, não aos falsos "amigos" que só são seus companheiros, quando vc tem algo á oferecer a eles.
Fertig
Internet
Start
ZoneAl... Eudora... Zone-H... Überse... Microso... D:\WIN... http://... hpG - ...
21:23

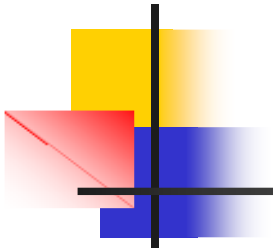
Rückblick 2003

Phishing

Einige bekannte Firmen sind hier betroffen gewesen:

- Banken wie die Citibank;
- Online-Firmen wie eBay und PayPal;
- Internet Service Providers wie AOL, MSN, Yahoo and EarthLink; Online-Shops wie Best Buy;
- Versicherungsagenturen

Phishing is a technique used to gain personal information for purposes of identity theft, using fraudulent e-mail messages that appear to come from legitimate businesses. These authentic-looking messages are designed to fool recipients into divulging personal data such as account numbers and passwords, credit card numbers and Social Security numbers.



IG:IS

Perimeterschutz

Ausgangslage:

- Internet ist DAS Medium geworden um den Geschäftsalltag zu erleichtern und zu optimieren, ABER auch die schädlichen Effekte.
- Einführung und Überwachung von Sicherheitssoftware wird ein fast unbewältigbarer Job bei steigender Anzahl von Computern.
- Die Sicherheitsprobleme werden immer vielfälltiger.
- Malware ist durch das Internet unheimlich schnell geworden.
- Alle hausinternen Informationen sind konzentriert auf EDV-Systemen gespeichert.
- Gesetzliche Vorgaben nehmen zu. (Datenschutz, Urheberrechtsschutz, ...)
- Die Zugänge zu den internen IT-Systemen haben zugenommen.
- Die Komplexität und die Anzahl der System steigt laufend!
- Neue Bedrohungen treten in immer kürzeren Abständen auf und sind immer effektiver.

Was ist im Moment als Schutz für EIN EDV-System notwendig!

- Datensicherung
- Laufendes Update des Betriebssystem und der sonstigen Software
- Schutz gegen Viren
- Schutz gegen Spam ("Stupid Person's Annoying Message")
- Personal-Firewall
- Dialer-Schutz
- Schutz gegen Spyware
- Verschlüsselung Daten
- Sicherstellen, dass nur berechtigte Personen Zutritt zu den Daten am Gerät erhalten.
- Sicherstellen, dass nur die notwendigen Berechtigungen erteilt sind.
- Mail-Client mit Verschlüsselungsmöglichkeit.
- Schutz der Daten gegen Diebstahl und Missbrauch
- Und alles weitere das ich als „Benutzer" nicht will

Genügt das alleine?

NEIN!

- 100% Sicherheit gibt es nicht
- Nur Systeme zum Schutz vor bekannten Schadensfunktionen einzusetzen, hilft nicht.
- Es ist notwendig zusätzlich den Ansatz zu verfolgen: Nur was für die jeweilige Tätigkeit unbedingt notwendig ist, ist verfügbar. (Programme und Daten)

-> **Restriktion = Risikominimierung**

Eingangspunkte ins Netz

- Wechselmedien
  - Diskette, CD/DVD-Rom, CD/DVD -Brenner
  - Zip
  - USB-Stick (Maus, Uhr)
  - Kartenleser
- Externe Speicher-Geräte mit Firewire, USB, IrDA, seriell, parallel, ...
  - Festplatte, CD, Diskette, ...
  - Digitalkamera
  - Handy
  - PDA
- Sonst. Netzwerkzugänge (Kabel oder Funk (Wlan, Bluetooth, IrDA))
- Modem
- Funkende Peripheriegeräte
- Internet (IP-Protokoll!)
- Usw.

Unser Lösungsansatz:

Lösungsansatz

- PC, Server, PDA sind gegen unerlaubte Konfigurations-Änderungen abgesichert.
- Netzwerk und deren Zugänge sind abgesichert. Nur ein definierter Kreis darf Änderungen vornehmen.
- Daten und Programme dürfen nur über definierte Schnittstellen die Unternehmensgrenze überschreiten. (z.B. Mail, Web, Speichermedien, ...) Der Rest ist deaktiviert.
- Verlassen Geräte mit Daten die physischen Unternehmensgrenzen so sind diese abgesichert.
- Erfolgt eine Kommunikation von internen Geräten über externe Kommunikationseinrichtungen so ist diese entsprechend abzusichern.

Schnittstellen

WEB:

- Firewall
- Proxy
  - 2 x Antivirus-Programm
  - Content-Filter
  - URL-Filter
  - Download-Filter
  - Log
- Intrusion-Detection/Prevention

Schnittstellen

Mail:

- Maileingangsserver
  - 2 x Antivirus-Programm
  - Content-Filter
  - SPAM-Schutz
  - Attachment-Block (Zumindest alles ausführbare!)
  - Log

Schnittstellen

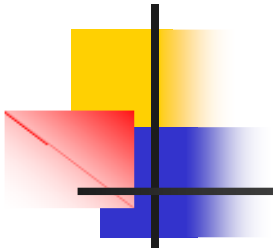
Speichermedien:

- Lokaler PC
  - Keine Zugriff auf externe Speichermedien
  - Ausgenommen Einschränkung auf definierte Übertragung
- Viren-Schleuse
  - 2 x Virenscanner
  - Log

IG:IS

Was gibt es noch zu bedenken:

- Verschlüsselung
- Digitale Kopierer
- Entsorgung von Datenträgern
- Output (Papier)
- Abstrahlung / Abhören
- Diebstahl von Hardware
- Spionage (Fotohandy)
- Tauschbörsen



IG:IS

Ausblick

2004

Ausblick 2004

"Zero-Day Attacks"

Sogenannte "Zero-Day Attacks" sind Angriffe, die Sicherheitslücken ausnützen, für die noch keine Patches zur Verfügung stehen. Hier ist die Vorbereitungszeit der Sicherheitsverantwortlichen gleich Null. Einer Umfrage von Computerworld auf der Info Sec 2003 zufolge werden diese Angriffe als wachsende Bedrohung angesehen.

SQL Slammer (Januar 2003)	8 Monate
Blaster (Sommer 2003)	1 Monat
Nachi/Welchi-Variante	1 Woche

Quelle: Computerwelt.de

Ausblick 2004

Schaden ist oft nicht mehr erkennbar

- Malware fällt immer weniger auf
- Die Schadensfunktion ist nicht mehr direkt erkennbar

ZIEL: Geld

Ausblick 2004

Aktuelle Viren 2004

Virus	Lokale Auffälligkeit	Schadens-funktion 1	Schadens-funktion 2	Schadens-funktion 3
Bagle	Keine			
Mydoom Novarg	Keine	Proxy	Backdoor	DoS
Mimail.q	Keine	Backdoor		
Dumaru	Keine	Backdoor	Keyboardlogger	

Rückblick 2004

Virenscanner Aktualisierungszeiten

	Erste Meldung	Update von Kaspersky	Trend Micro	Symantec	Sophos	McAfee	Differenz
Xombe	08.01.2004 23:26	09.01.2004 11:15	09.01.2004 17:40	09.01.2004 22:30	09.01.2004 15:30	14.01.2004 22:50	5 Tage
Bagle	18.01.2004 11:36	18.01.2004 14:50	19.01.2004 03:00	19.01.2004 06:05	19.01.2004 03:00	19.01.2004 06:20	15:30 Stunde
Dumaru.Y	N/A	24.01.2004 11:20	24.01.2004 22:20	27.01.2004 01:05	24.01.2004 20:30	26.01.2004 17:40	3 Tage
Mydoom (EXE)	N/A	27.01.2004 00:30	26.01.2004 23:35	27.01.2004 01:05	27.01.2004 01:40	27.01.2004 05:00	05:25 Stunde
Mydoom (DLL)	N/A	27.01.2004 04:35	26.01.2004 23:35	27.01.2004 04:35	27.01.2004 01:40	27.01.2004 05:00	05:25 Stunde

Dies stellt nur einen kleinen Ausschnitt der Produkte und der dokumentierten Zeiten dar.
Quelle: PC-Welt/www.av-test.org

Das war der 1. Erfahrungsaustausch!

- Fragen
- Anregungen
- Tipps
- Wünsche

Ein Gedanke auf den Weg....

Security is not a goal, it is a process,

Security is not a product, it is a mindset.

Security is a never ending task.

If you think you are secure...

Just wait a few minutes until the next exploit is released.

Security is like breathing -

You must not stop.