Rozwiązania antywirusowe H+BEDV dla serwerów Linux, FreeBSD i innych platform

CC Otwarte Systemy Komputerowe Sp z o.o.

http://www.cc.com.pl/

Rakowiecka 36, 02-532 Warszawa

Grzegorz.Blinowski@cc.com.pl

tel. +48 22 646-6873 fax. +48 22 606-3780

http://www.hbedv.com/

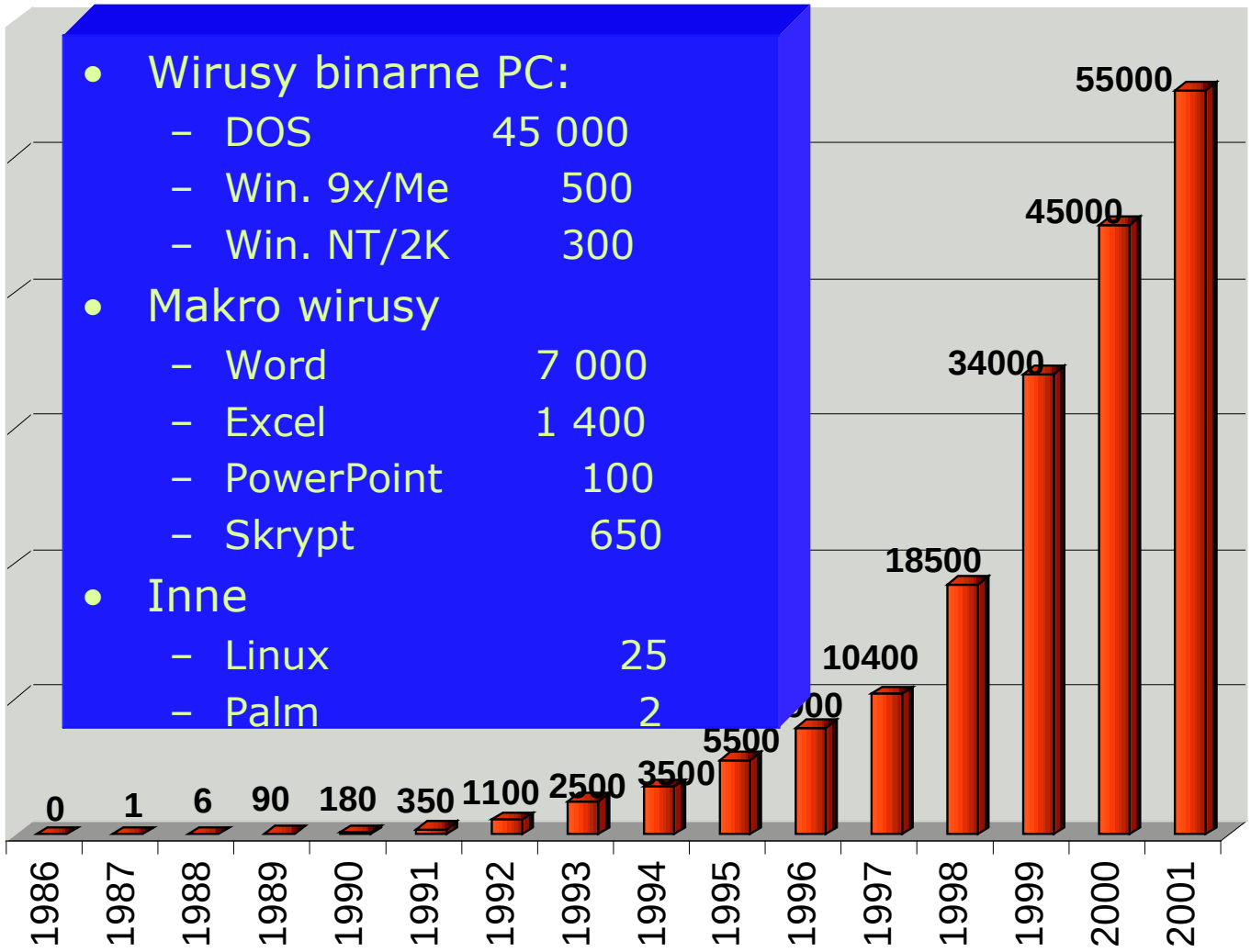
Co to jest CC?

- **CC Otwarte Systemy Komputerowe** działa od 1995 r. (sp. z o.o. od 2001)
- Oferujemy:
  - Rozwiązania z dziedziny bezpieczeństwa sieci komputerowych
  - Produkcja własnego, wyspecjalizowanego oprogramowania
- Afiliacje:
  - CheckPoint
  - CLEARSWIFT
  - H+BEDV
  - Netscreen
  - Sun.One (iPlanet, Netscape)
  - SUN Microsystem
  - Vasco,
  - StoneSoft

http://www.hbedv.com/

Współczesne zagrożenia

- Wirusy binarne PC:
  - DOS 45 000
  - Win. 9x/Me 500
  - Win. NT/2K 300
- Makro wirusy
  - Word 7 000
  - Excel 1 400
  - PowerPoint 100
  - Skrypt 650
- Inne
  - Linux 25
  - Palm 2



http://www.hbedv.com/

AntiVir®

CC Otwarte Systemy Komputerowe Sp. z o.o.

Współczesne zagrożenia

Wektory:

- Załączniki E-mail (80%)
- Pliki pobierane z WWW
- Usenet News
- IRC
- P2P (np. Gnutella)
- ICQ / IM
- piracki CD-ROM
- IRDA
- Demo CD-ROM

- 1998: CIH
- 1999: Melissa
- 2000: Love Letter
- 2001: Code Red
- 2001: Nimda
- 2002: Klez
- 2003: Slammer
- 2003: Blaster

AntiVir®

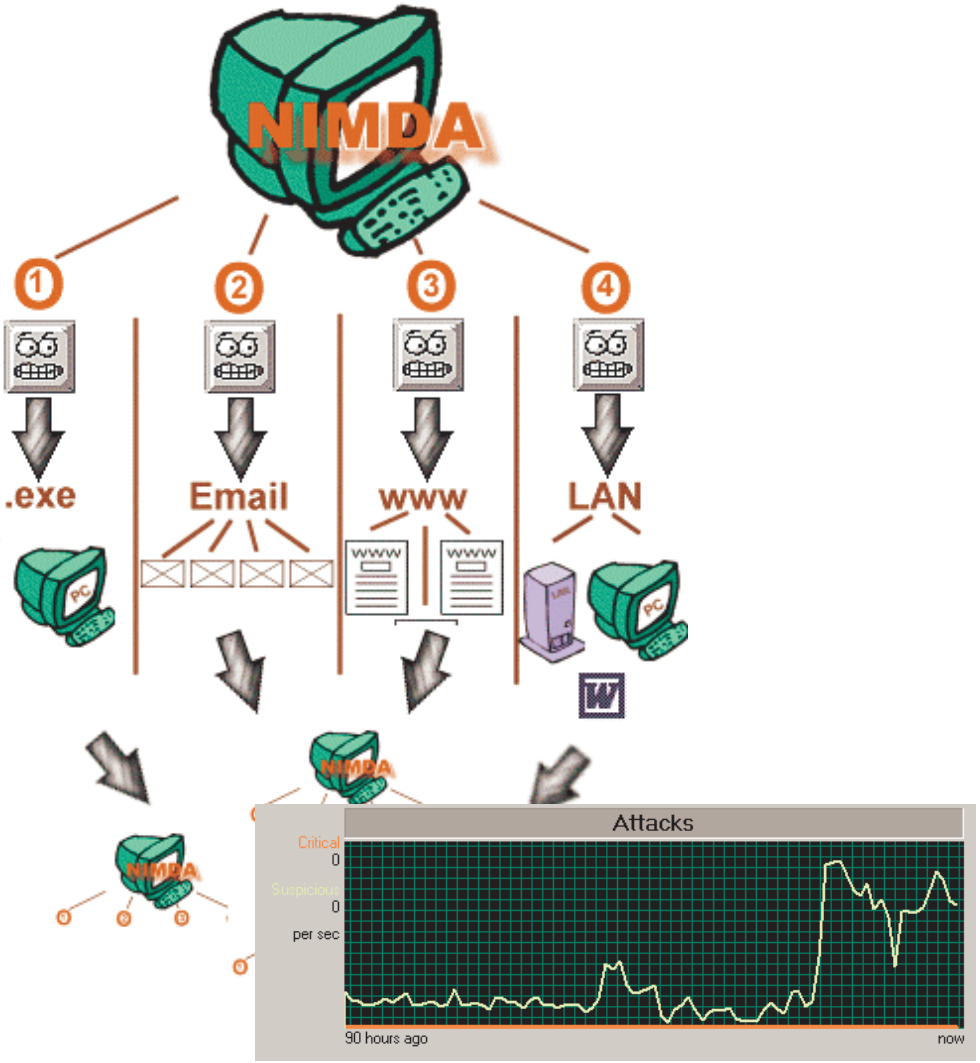
CC Otwarte Systemy Komputerowe Sp. z o.o.

Współczesne zagrożenia

- Hybrydy: wirus-robak (Melissa, BadTrans, Klez)
  - wektor e-mail z wykorzystaniem aplikacji biurowych
- DoS (Denial of Service) i DDoS (Distributed Denial of Service) - jako efekt uboczny(?)
  - Slammer, Blaster
- Wykorzystanie dziur w WWW i innych serwisach sieciowych
  - Code Red (WWW)
  - Slammer (SQL)
  - Blaster (RPC)

Przykład - "Nimda"

- "4 wirusy w jednym"
- wektor - e-mail
- atakuje dostępne dyski sieciowe, udostepnia publicznie dysk C:
- atakuje serwer WWW Microsoft (IIS)
- Dokleja się do plików na lokalnym i zdalnych dyskach



http://www.hbedv.com/

Przykład - "Slammer"

- Początek rozprzestrzeniania się: sobota 24.01.2003, godz 07:31
- Wykorzystuje znaną wcześniej dziurę w Microsoft SQL Server / MSDE 2000
- W skali Internet generuje gigantyczny ruch:
  - 100 000 zainfekowanych maszyn
  - Lawinowy wzrost liczby pakietów w 3 minuty
  - Podwajanie liczby zainfekowanych maszyn co 8,5 s.
  - Jedna maszyna może teoretycznie zainfekować 30 000 następnych w ciągu sekundy

Niektóre szkody:

- Zamknięcie sieci ATM Bank of America na 2 dni
- Wyłączenie numeru 911 w Seattle
- Odłączenie Korei Pd. i Słowenii od Internetu

http://www.hbedv.com/

AntiVir®

CC Otwarte Systemy Komputerowe Sp. z o.o.

Przykład - "Blaster"

- Rozprzestrzenia się dzięki dziurze w Microsoft DCOM RPC (port 135 TCP - otwarty na praktycznie każdej maszyni Win NT/2K/XP)
- Atak następuje poprzez przesłanie jednego pakietu (podobnie jak dla Slammer-a)
- Przeprowadza atak DoS na **windowsupdate.com** - 50 pseudo-sesji ht / sekundę
- średni czas "życia" systemu bez poprawek podłączonego do TPNET (0202122) wynosi ok. 60 s
- Tworzy zdalny nasłuchujący cmd.exe na TCP 4444

I just want to say LOVE YOU SAN!! billy gates why do you make this possible ? Stop making money and fix your software!!

http://www.hbedv.com/

AntiVir®

CC Otwarte Systemy Komputerowe Sp. z o.o.

Rynek systemów antywirusowych

http://www.hbedv.com/

Rynek systemów antywirusowych

- Kilkunastu producentów o zasięgu globalnym
- Typowo - jeden producent "lokalny"
- Kilku-kilkunastu producentów rozwiązań niszowych

http://www.hbedv.com/

AntiVir®

CC Otwarte Systemy Komputerowe Sp. z o.o.

Aladdin	eSafe
Alwil Software, DCA	avast!
Cat Computer Services	QuickHeal
Central Command	Vexira
Command Software, perComp Verlag	Command AV
Computer Associates	eTrust EZ AV
Computer Associates	InoculateIT
Computer Associates	VET AV
Cybersoft	Wave AV, VFind
Eset	NOD 32
F-Secure	F-Secure AV 5
F-Secure, perComp Verlag	F-Secure AV 4
Finjan Software	SurfinGate
Frisk Software	F-Prot
Frisk Software, DTP Neue Medien	FP-WIN Professional
Frisk Software, perComp Verlag	FP-WIN Anti-Virus
G Data	AntiVirenKit
GeCAD	Reliable AV (RAV)
Grisoft, Jakob Software	AVG
Group Technologies	securiQ.Watchdog
H+BEDV Datentechnik	AntiVir
H+BEDV Datentechnik	AntiVir Personal Edition
Ikarus Software	Virus Utilities, Content Wall
Kaspersky Lab, DATSEC	Kaspersky AV
MicroWorld, MAXXdefense	eScan, MailScan
Mitcom	Dr. Web, Anti-Viren-Pack
MKS	MKS_Vir
Network Associates	Dr. Solomon's AVTK
Network Associates	McAfeeVirusScan (Retail)
Network Associates	Virusscan, Netshield
Norman Data Defense	Virus Control
Norman Data Defense	Virus Control Home
Omegas	Dr. Turbo Anti-Virus
Panda Software	Panda AntiVirus
Softwin	Bitdefender
Sophos	Sophos AntiVirus, Mail Monitor
Sybari, Infowan	Antigen
Symantec	Anti-Virus Solution
Symantec	Norton AntiVirus
Trend Micro	OfficeScan, ServerProtect
Trend Micro	PC-Cillin
VirusBuster	VirusBuster

http://www.hbedv.com/

AntiVir®

CC Otwarte Systemy Komputerowe Sp. z o.o.

Charakterystyka systemów AV

- Indywidualne, "personalne" - na biurko
  - większość producentów
- Dla użytkowników w korporacjach
  - producenci "rozwiązań korporacyjnych"
- Bramki SMTP, WWW:
  - autonomiczne
  - współpracujce z programami "Content Security" (CheckPoint, Netscreen, Clearswift, ...)
- Dedykowane do aplikacji
  - np. dla Exchange, Domino, itp.
- Skanery sprzętowe
  - urządzenia bazujące na maszynach typu PC
  - rozwiązania "naprawde sprzętowe", tj. wyszukiwanie wzorców wirusów wspomagane hardwarowo

http://www.hbedv.com/

AntiVir®

CC Otwarte Systemy Komputerowe Sp. z o.o.

Cechy systemów AV

- Skanowanie plików i operacji we/wy
- Skanowanie ruchu sieciowego (desktop, serwer)
- Centralne: zarządzanie, konfiguracja, dystrybucja
- Funkcje dodatkowe, typowe dla programów Content Security, np. Anty-spam

http://www.hbedv.com/

AntiVir®

CC Otwarte Systemy Komputerowe Sp. z o.o.

Trendy

- Funkcjonalne zróżnicowanie oferty:
  - oferowanie rozwiązań serwerowych i filtrujacych ruch sieciowy
- Platformowe zróżnicowanie oferty
  - wersje dla systemów Unix (zwłaszcza Linux)
- Rozwiązania "prawdziwie sprzętowe" - np. Rad, Fortinet, ...
- AV staje się częścią szerszej gamy rozwiązań ContentSecurity:
  - dołączenie funkcji takich jak: antyspam, blokowanie aplikacji, itp. <- Konwergencja AV - CS

AntiVir®

CC Otwarte Systemy Komputerowe Sp. z o.o.

H+BEDV Datentechnik:

Firma i Rozwiązania

http://www.hbedv.com/

AntiVir®

CC Otwarte Systemy Komputerowe Sp. z o.o.

H+BEDV - firma

- Największy niezależny producent oprogramowania antywirusowego w Niemczech
- Założenie: 1988 - 15 lat na rynku
- Produkty dla: stacji roboczych, serwerów, serwerów E-mail, innych platform oraz engine AV w wersji OEM
- Darmowa wersja desktop dla użytkowników indywidualnych
- Kilka milionów sprzedanych licencji

http://www.hbedv.com/

AntiVir®

CC Otwarte Systemy Komputerowe Sp. z o.o.

H+BEDV - firma

1988 Jeden z pierwszych programów AV

1993 Opracowanie AVScan

1994 AV dla NetWare i Windows

1998 Pierwsza licencja "Campus"

1999 Program rezydentny

2000 AntiVir MailGate

2001 AntiVir dla Windows XP

2002 AntiVir Rescue System

2003 AntiVir WebGate, F-1

http://www.hbedv.com/

AntiVir®

CC Otwarte Systemy Komputerowe Sp. z o.o.

H+BEDV Technologia

- Jeden przenośny "engine" dostępny dla różnych platform
- Heurystyczne wykrywanie makro-wirusów
- Automatyczny update on-line
- Rozpoznawanie i skanowanie archiwów z konfigurowanym poziomem zagnieżdżenia
- Wydajna architektura

http://www.hbedv.com/

AntiVir®

CC Otwarte Systemy Komputerowe Sp. z o.o.

H+BEDV Produkty

- Stacje robocze
  - Windows 9x/ME, NT, 2000, XP
  - Windows 3.11
  - DOS, OS/2
  - Linux
- Serwery plików
  - Linux
  - FreeBSD, OpenBSD
  - Windows
  - Novell Netware
- Serwery E-mail
  - Linux i *BSD
  - sendmail, postfix, inne
- WWW
  - autonomiczne proxy WebGate - Linux
- Checkpoint Firewall-1
  - F-1 - zgodny z OPSEC CVP
- Engine w wersji OEM - Linux demon

http://www.hbedv.com/

AntiVir®

CC Otwarte Systemy Komputerowe Sp. z o.o.

H+BEDV: AV dla serwerów plików

- Platformy: Linux, FreeBSD, OpenBSD, Windows, Novell Netware
- Praktycznie "nieczułe" na dystrybucję Linuxa: Red Hat, SuSE, SlackWare, … - wymagania wył. do wersji jądra systemu
- Cechy:
  - stałe monitorowanie
  - update on-line
  - monitorowane operacji we/wy
  - konfigurowalna reakcja na wykrycie wirusa
  - wysyłanie ostrzeżeń
- Licencjonowanie:
  - per server, niezależne od liczby użytkowników

http://www.hbedv.com/

AntiVir®

CC Otwarte Systemy Komputerowe Sp. z o.o.

H+BEDV: AV dla serwerów plików

- Wszystkie systemowe operacje na plikach przechwytywane przez specjalny driver systemowy (Windows, Novel)
- Linux, FreeBSD, OpenBSD - funkcje systemowe open(), close(), exec() przechwycone przez moduł "Dazuko"
  - oprogramowanie open source sponsorowane przez H+BEDV
  - rejestracja zmian zachodzących w określonych plikach/katalogach i powiadamianie nadzorującej aplikacji
  - funkcjonuje także dla plików sieciowych (NFS, samba)
  - **http://www.dazuko.org/**

http://www.hbedv.com/

AntiVir®

CC Otwarte Systemy Komputerowe Sp. z o.o.

Dazuko

registration function

```
int dazukoRegister(const char *groupName);
```

configuration functions

```
int dazukoSetAccessMask(unsigned long accessMask);
int dazukoAddIncludePath(const char *path);
int dazukoAddExcludePath(const char *path);
int dazukoRemoveAllPaths(void);
```

file access control functions

```
int dazukoGetAccess(struct access_t *acc);
int dazukoReturnAccess(struct access_t *acc);
```

unregistration function

```
int dazukoUnregister(void);
```

access structure

```
struct access_t
{
int deny;       int event;
int o_flags;    int o_mode;
int uid;        int pid;
char filename[4095]; };
```

http://www.hbedv.com/

AntiVir®

CC Otwarte Systemy Komputerowe Sp. z o.o.

H+BEDV: AV dla serwerów E-mail

- Platformy: Exchange, Linux, FreeBSD, OpenBSD
- Praktycznie "nieczułe" na dystrybucję Linuxa: Red Hat, SuSE, SlackWare, ...
- Cechy:
  - skanowanie on-line przechodzącej poczty SMTP
  - update on-line
  - konfigurowalna reakcja na wykrycie wirusa
  - wysyłanie ostrzeżeń e-Mail
  - skanowanie i naprawa załączników

http://www.hbedv.com/

H+BEDV: AV dla serwerów E-mail

- Integracja:
  - funkcjonuje jako niezależny relay SMTP
  - funkcjonuje także jako skaner AV bezpośrednio zintegrowany z serwerem E-mail:
    - Postfix,
    - Qmail,
    - Exim
    - sendmail
    - BenHur*

  - Powiadamianie nadawcy i/lub odbiorcy w wypadku wykrycia wirusa

http://www.hbedv.com/

AntiVir®

H+BEDV: WebGate - AV dla WWW

CC Otwarte Systemy Komputerowe Sp. z o.o.

- Platformy: Linux
- Praktycznie "nieczułe" na dystrybucję Linuxa: Red Hat, SuSE, SlackWare, ...
- Cechy:
  - autonomiczne proxy WWW z wbudowanym skanerem
  - skanowanie on-line ruchu http oraz ftp/http
  - update on-line
  - konfigurowalna reakcja na wykrycie wirusa
  - kontrola załączników w WebMail
- Konfiguracja, monitorowanie:
  - command-line, konsola Java

http://www.hbedv.com/

AntiVir®

CC Otwarte Systemy Komputerowe Sp. z o.o.

H+BEDV: inne produkty AV

- Antivir For MIMEsweeper
  - Skaner AV przeznaczony dla oprogramowania Content Security firmy Clearswift: MAILsweeper for SMTP oraz MIMEsweeper for WEB
- Antivir F-1
  - Moduł zgodny z CheckPoint OPSEC CVP przeznaczony dla firewall-i firmy CheckPoint (i innych zgodnych z OPSEC)
- Antivir OEM
  - Wersja OEM w postaci demona dla systemu Linux + SDK

http://www.hbedv.com/

AntiVir®

CC Otwarte Systemy Komputerowe Sp. z o.o.

Partnerzy

http://www.hbedv.com/

AntiVir®

CC Otwarte Systemy Komputerowe Sp. z o.o.

Certyfikaty i organizacje

http://www.hbedv.com/

AntiVir®

CC Otwarte Systemy Komputerowe Sp. z o.o.

Nagrody i wyróżnienia

http://www.hbedv.com/

Dystrybucja w Polsce

CC Otwarte Systemy Komputerowe Sp z o.o.

http://www.cc.com.pl/

Rakowiecka 36, 02-532 Warszawa

tel. +48 22 646-6873

fax. +48 22 606-3780

http://www.hbedv.com/

AntiVir®

CC Otwarte Systemy Komputerowe Sp. z o.o.

Pytania?

http://www.hbedv.com/