

Tendenser och intryck utifrån Sitics verksamhet

Nätverkssäkerhet 2003, läge och trender
Internetdagarna 2003



POST & TELESTYRELSEN

Presentationssstruktur

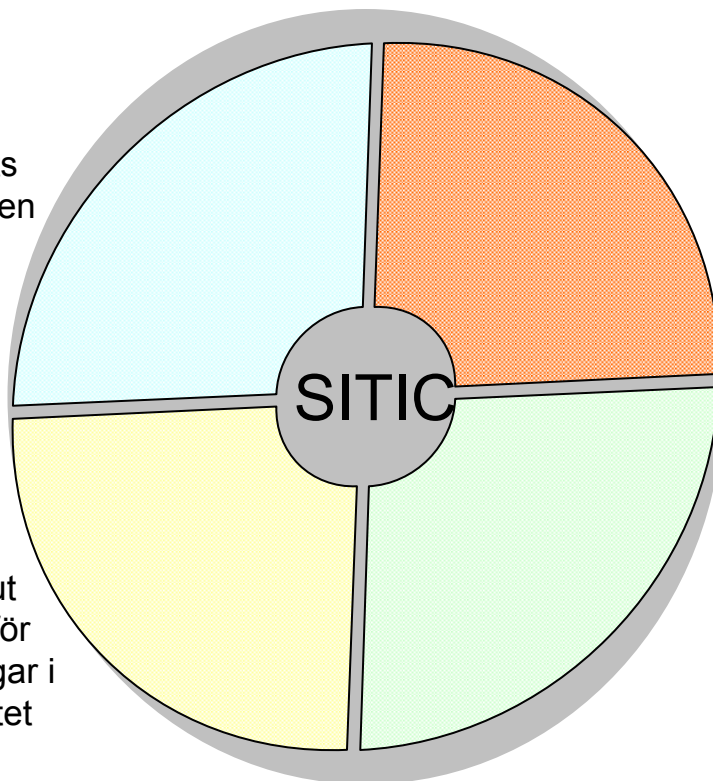
- Kort om Sitic
- Externa källor
- Sitic statistik
- Förklaringar
- Hotet – hackare eller användare?
- Vägen framåt

PTS uppdrag

Stödja samhället i arbetet med skydd mot IT-incidenter genom att:

Inrätta ett system för informationsutbyte om IT-incidenter mellan samhällets organisationer och funktionen

Snabbt kunna sprida information i samhället om nya problem som kan störa IT-system



Sammanställa och ge ut statistik som underlag för kontinuerliga förbättringar i det förebyggande arbetet

Lämna information och råd om förebyggande åtgärder

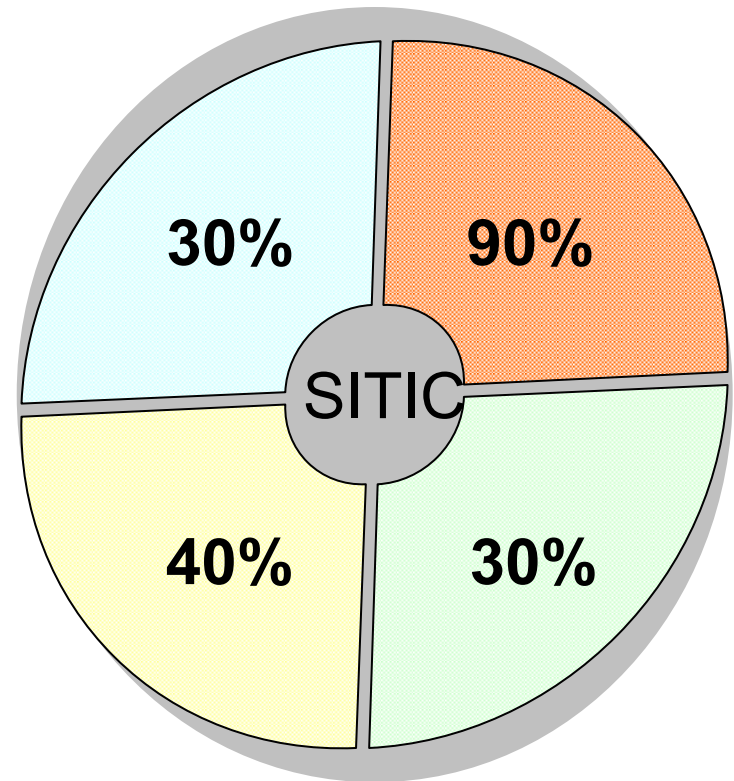
Inrättad 31 december 2002



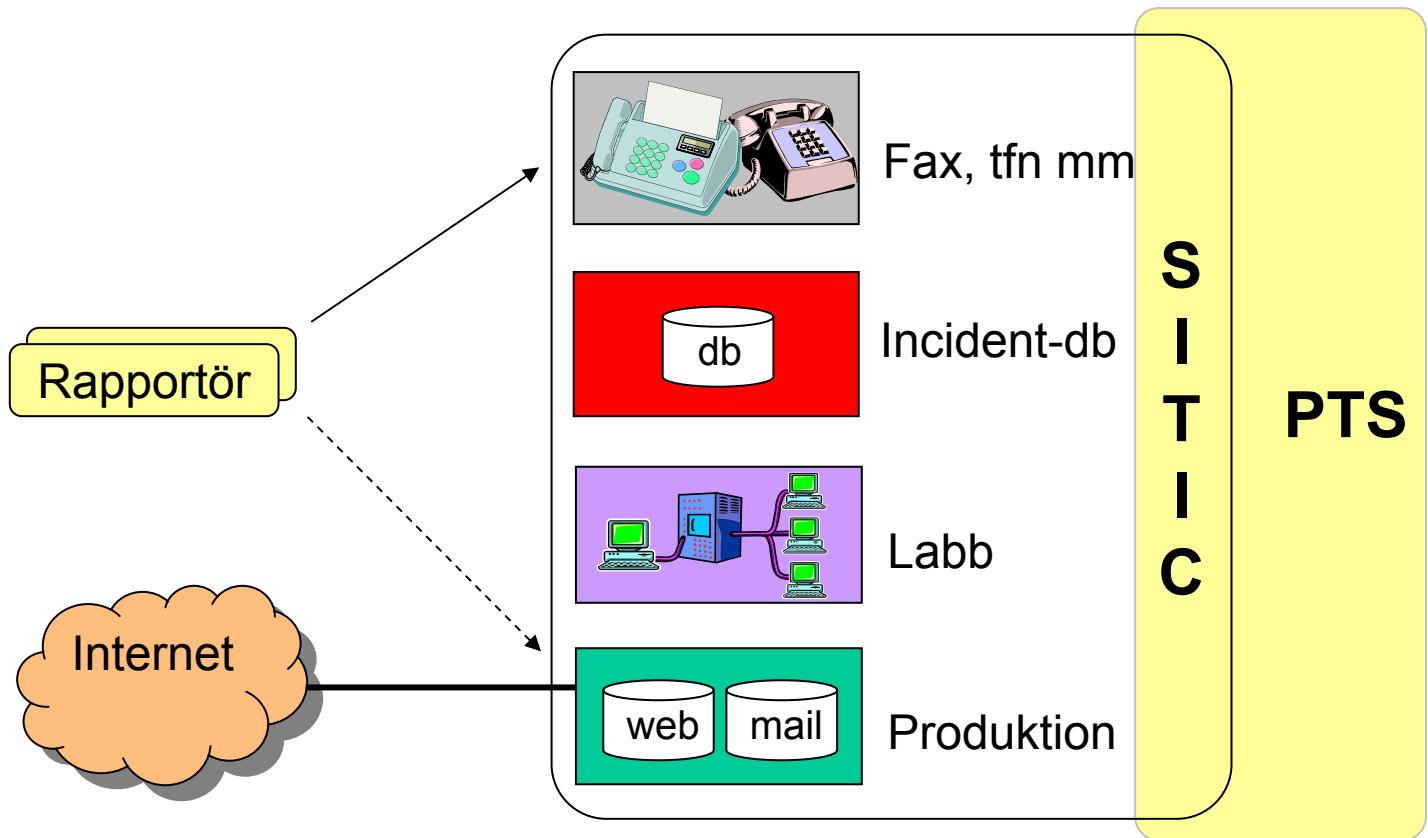
POST & TELESTYRELSEN

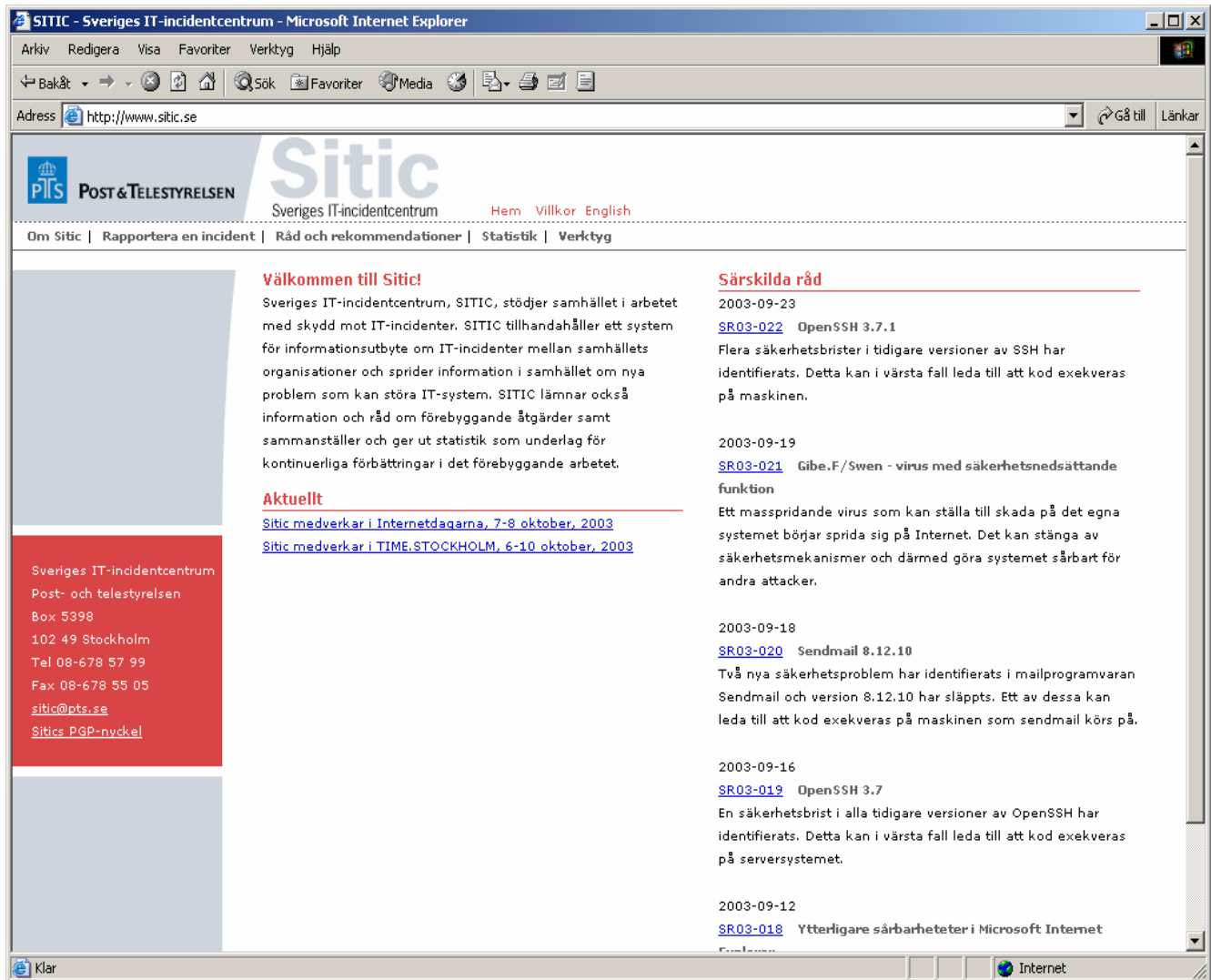
Nuläge

- I drift sedan 2003-01-02
- Stegvis införandeplan
 - Anslutning av bevakningsmyndigheter
 - Utveckling av kontakter med andra IT-incidentfunktioner, myndigheter, företag och organisationer
 - Implementering och utveckling av arbetsmetoder och samverkansformer
- Förslag till ändring av sekretesslagen
- Vidareutveckling av produktions- och labbmiljö
- Ytterligare rekrytering

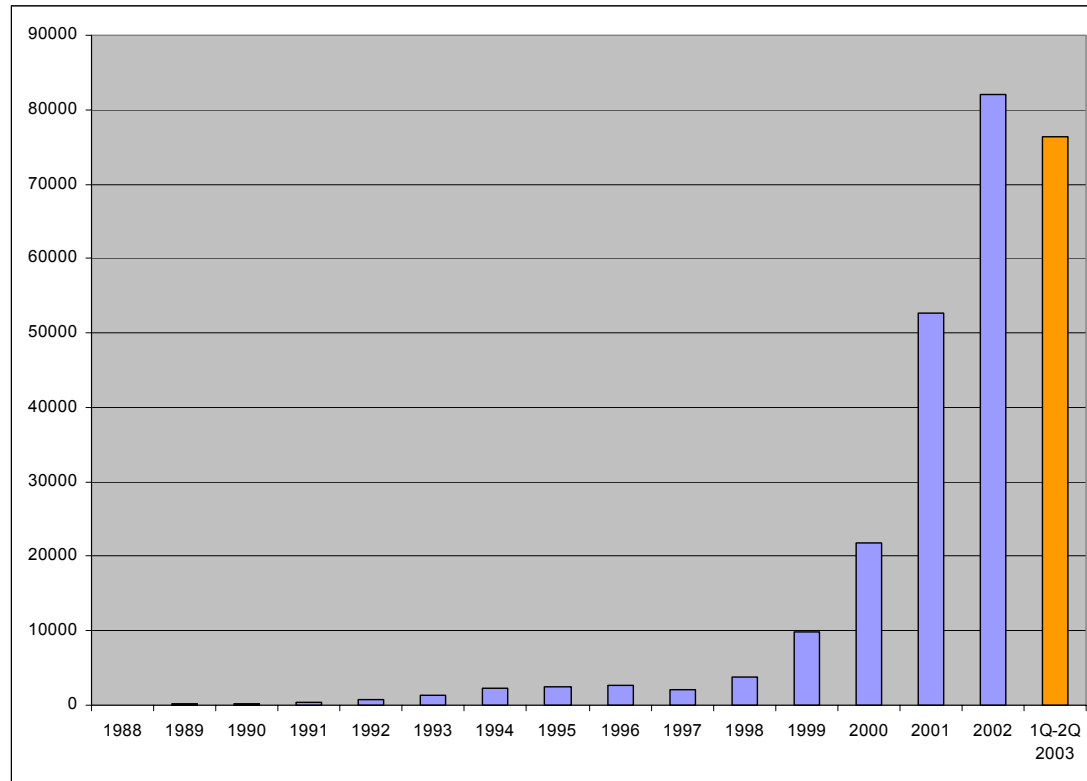


Fysisk och teknisk miljö

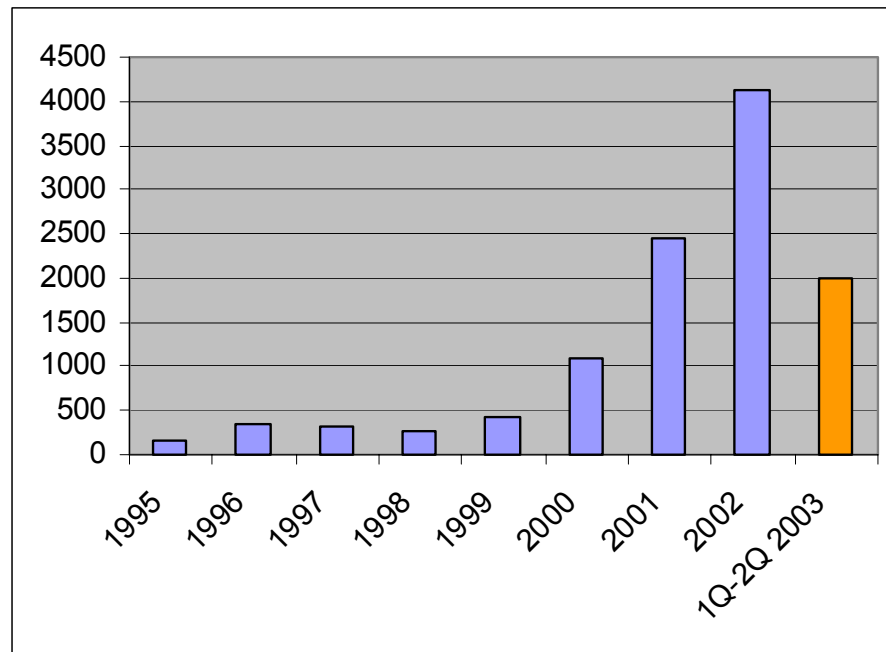




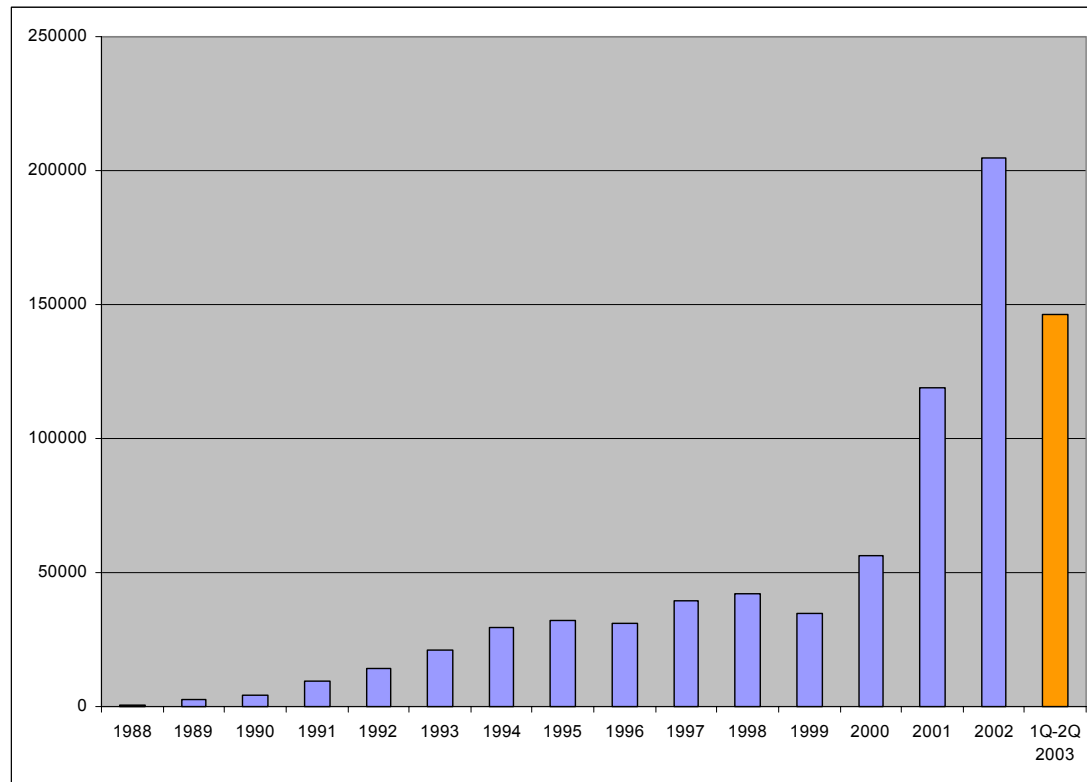
CERT/CC: Antal incidenter



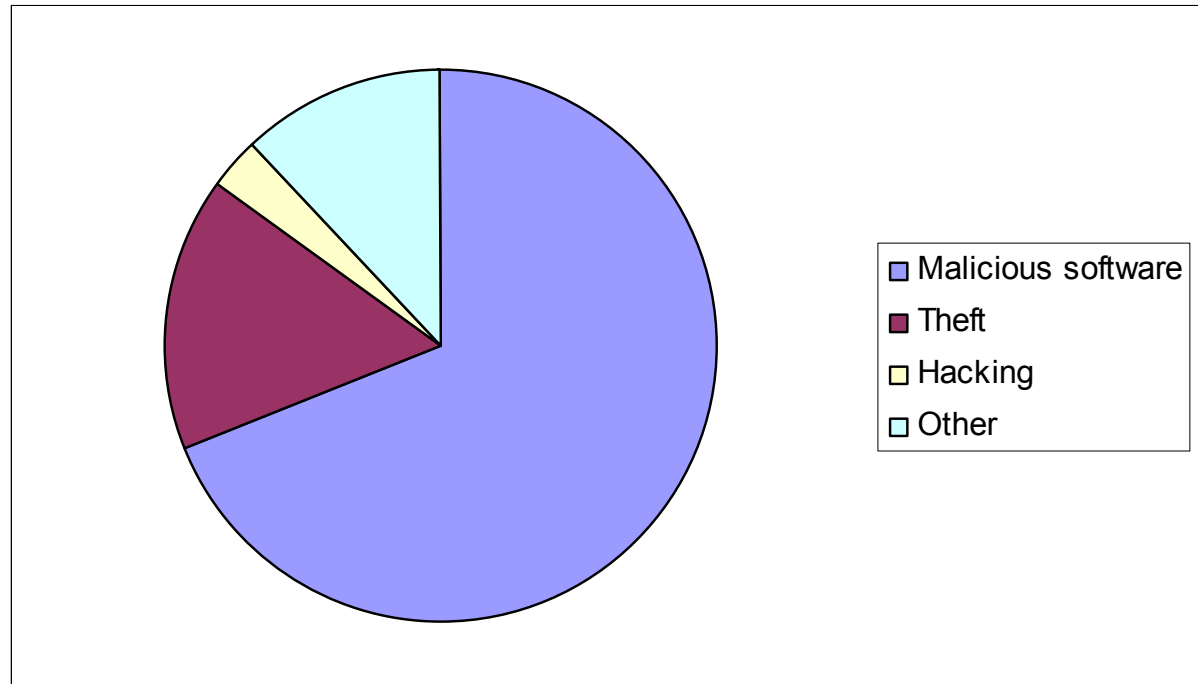
CERT/CC: Antal sårbarheter



CERT/CC: Inkommen e-post

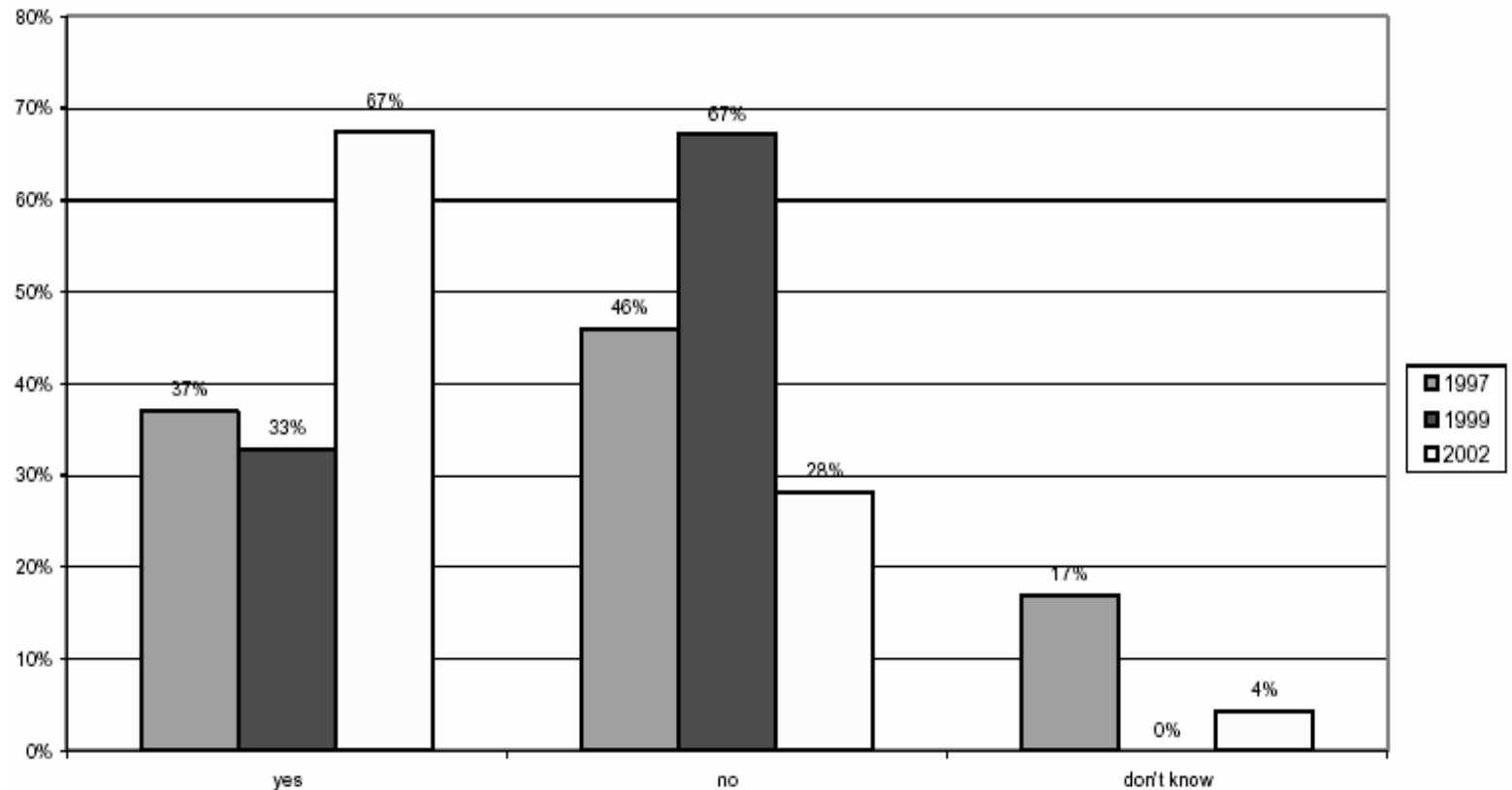


UNIRAS: Incidenttyp 2001-2002

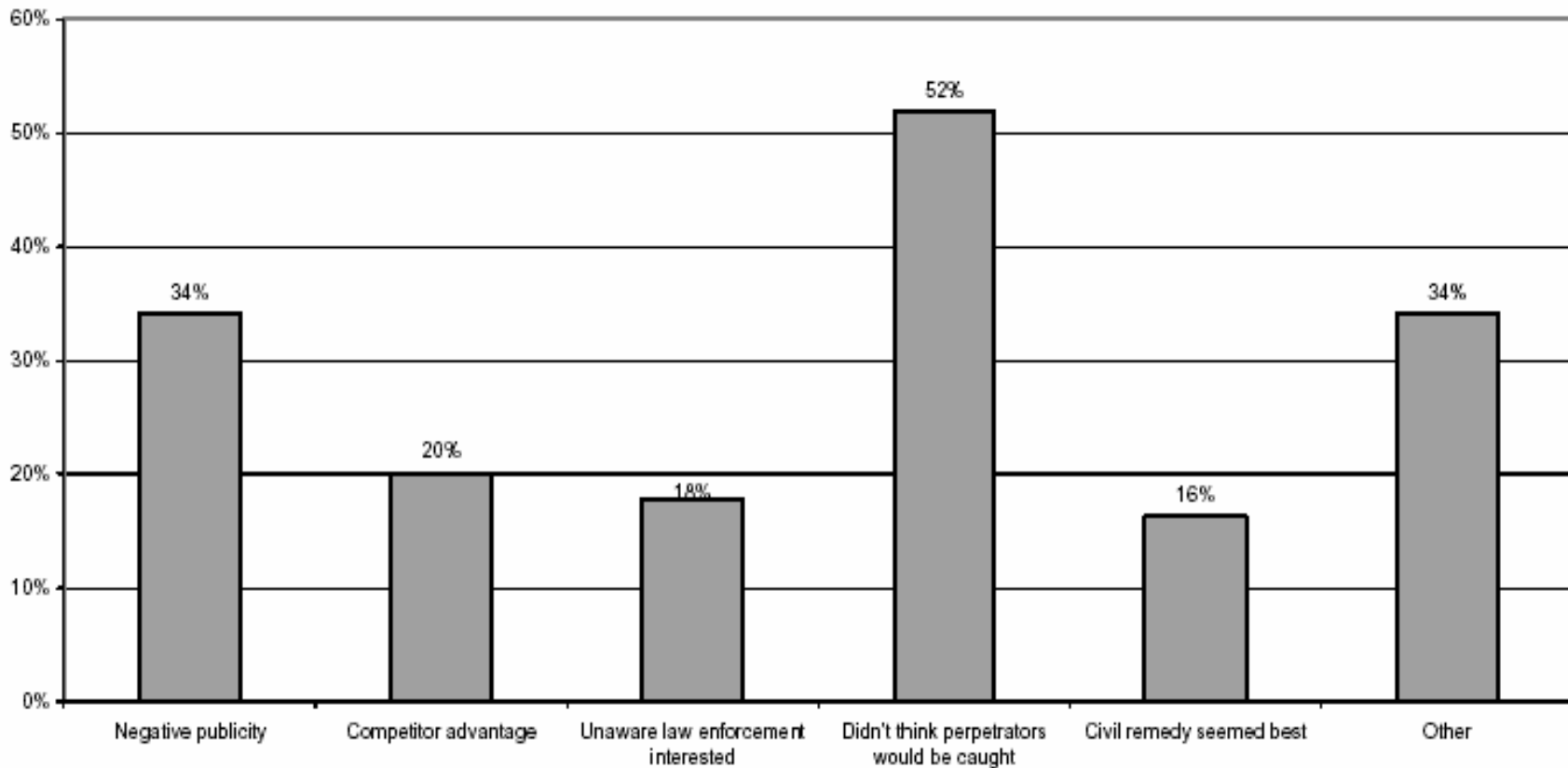


AusCERT: Incidentprofil

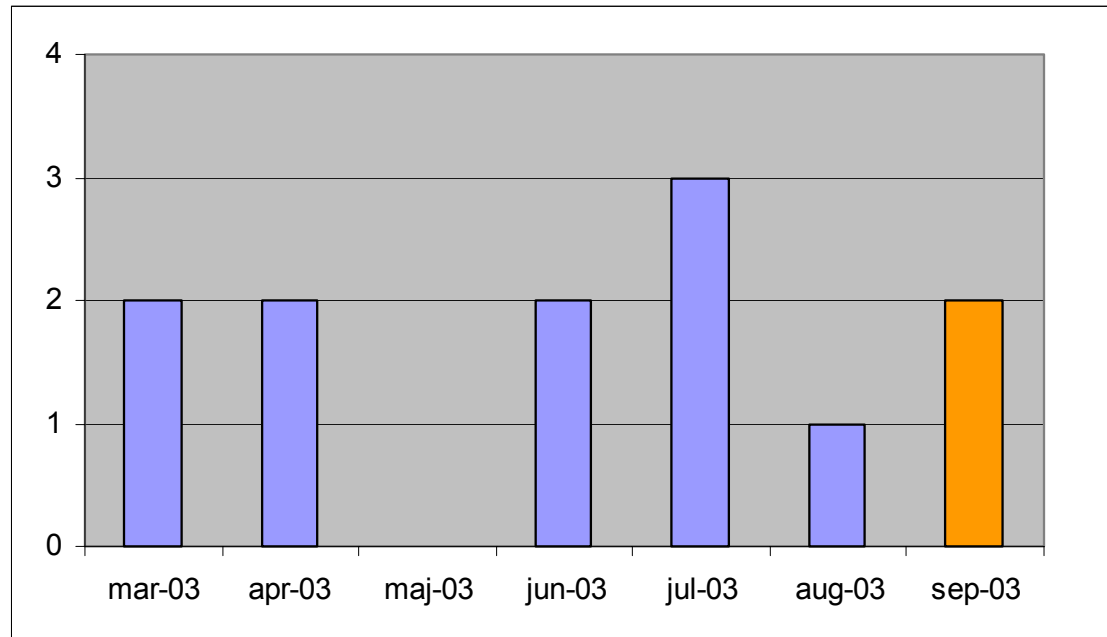
Upplevt attacker senaste 12 mån?



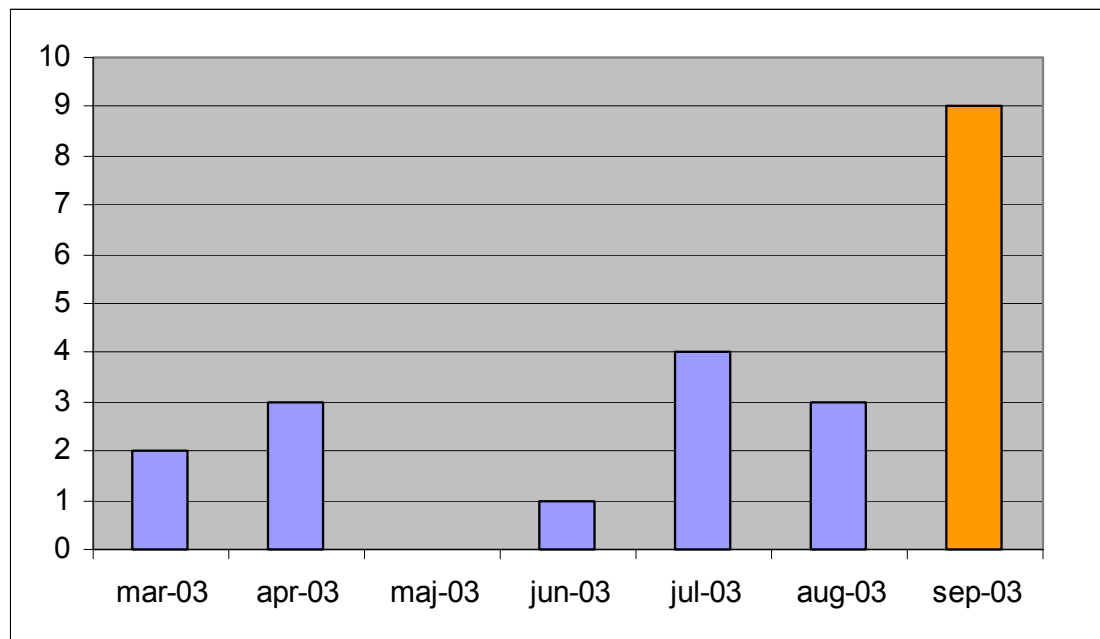
AusCERT: Skäl till utebliven rapportering



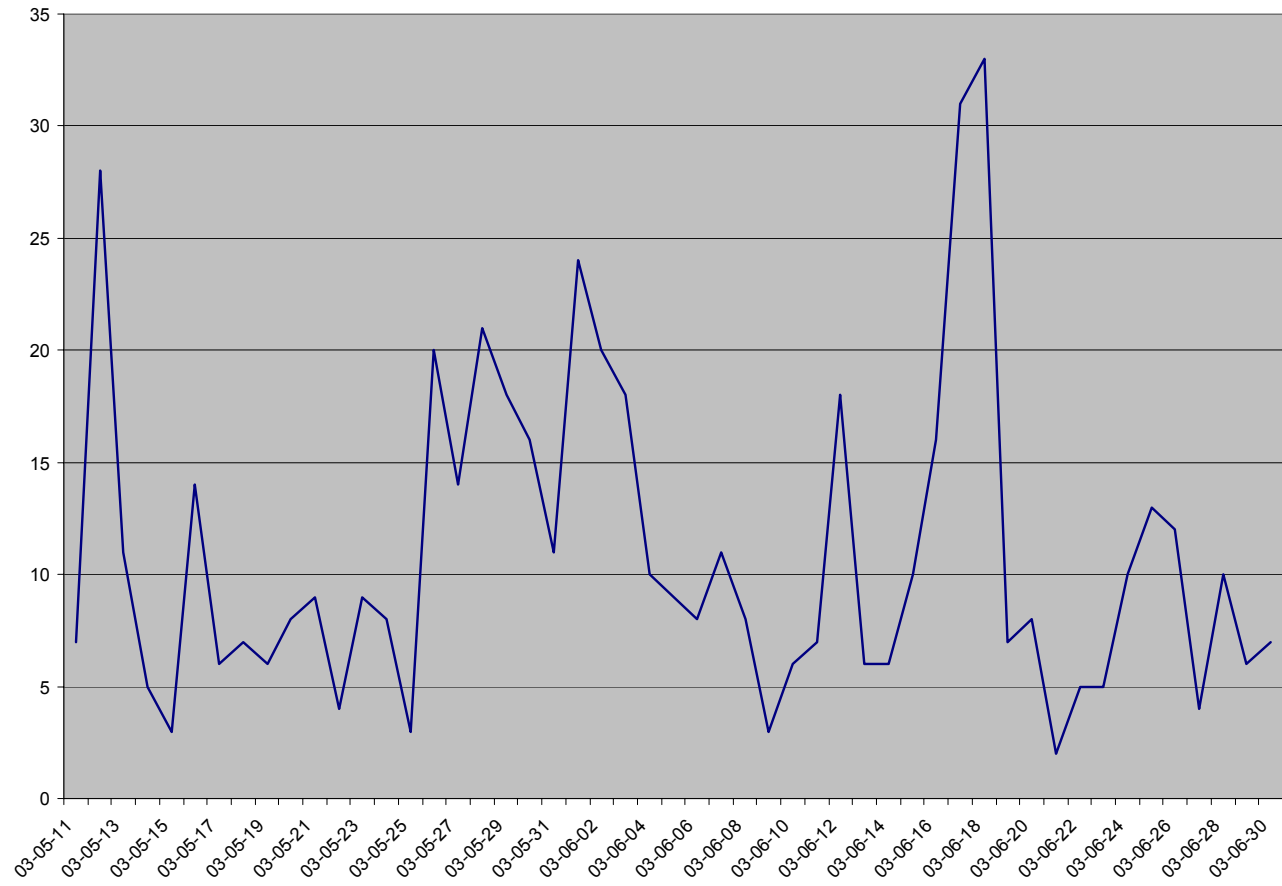
Sitic: Blixtmeddelanden 2003



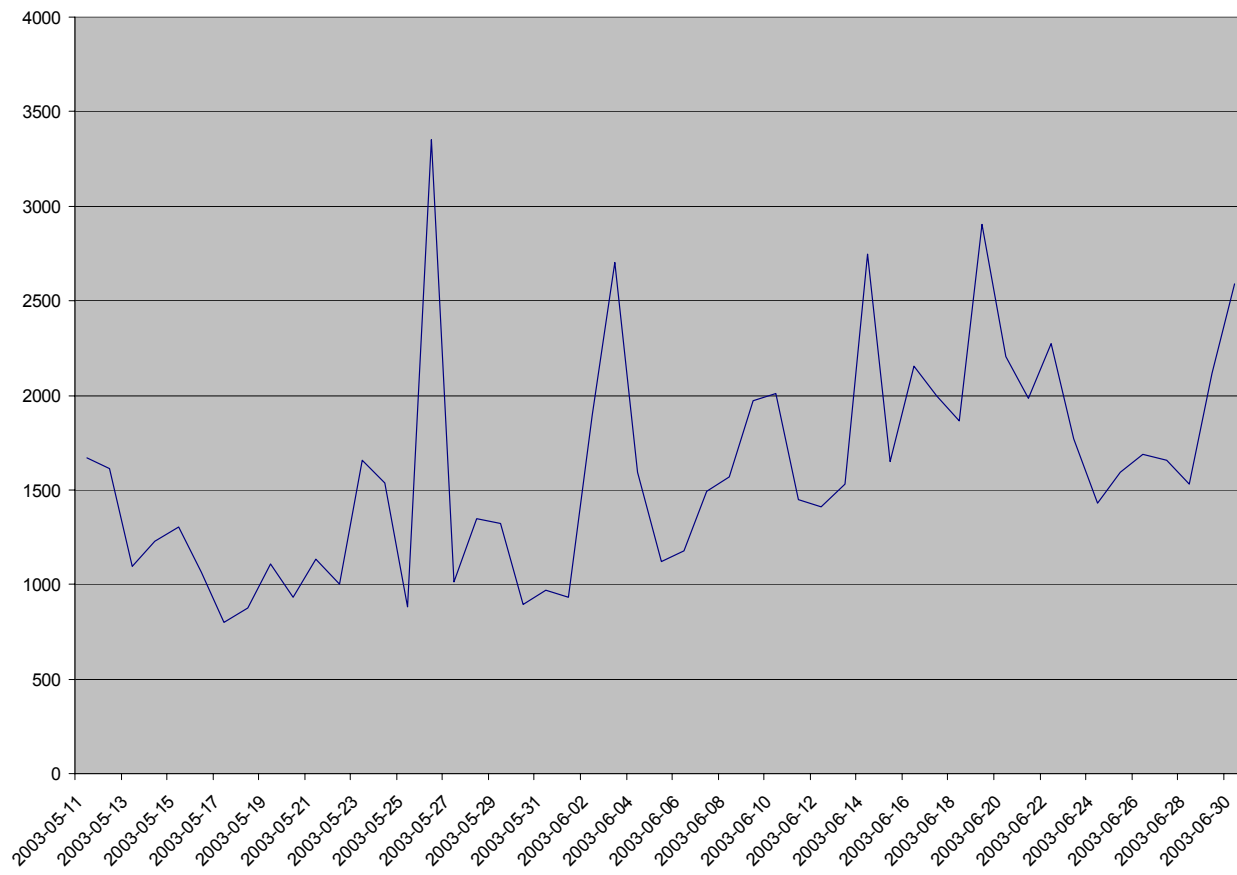
Sitic: Särskilda Råd 2003



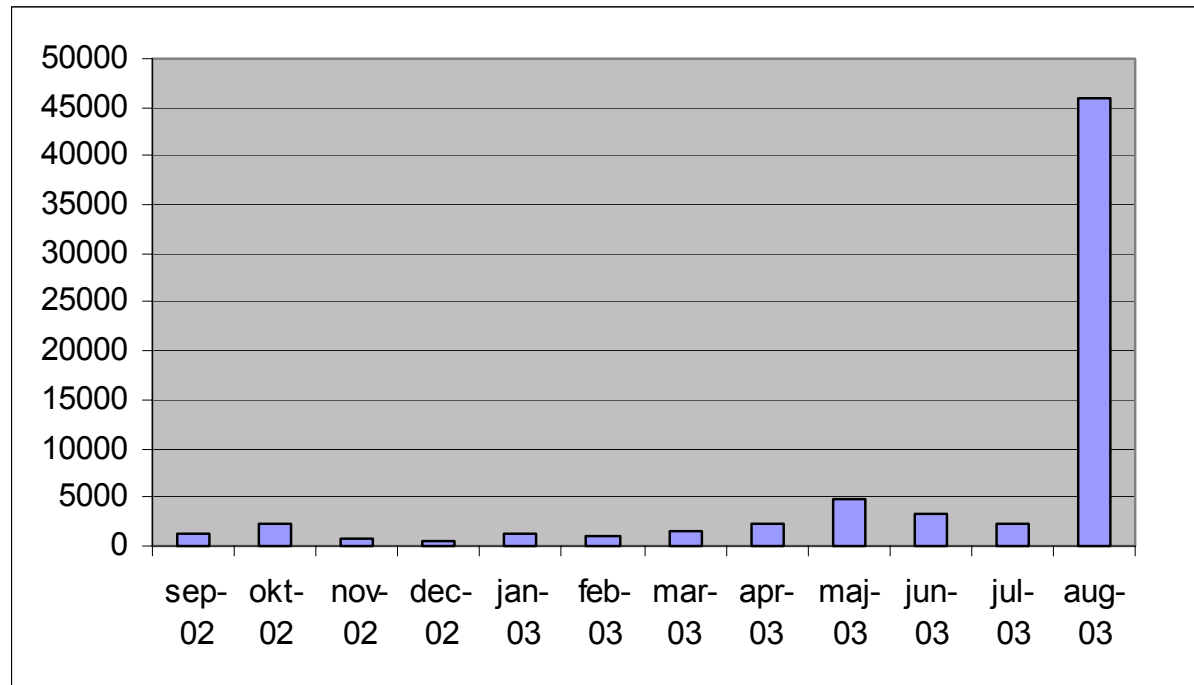
Sitic: Unika avsökningskällor / dag



Sitic: Slammer / Sapphire (period)

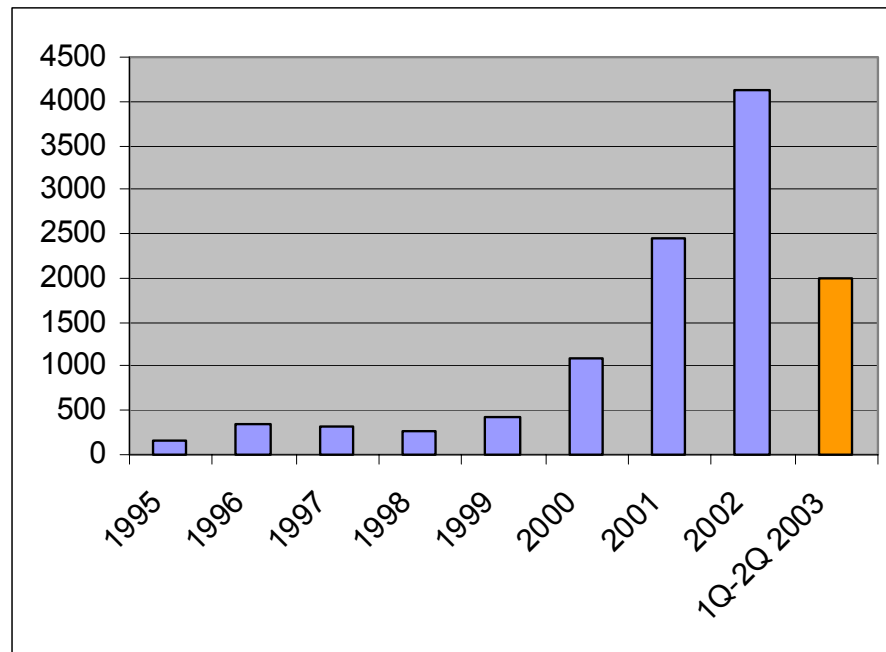


Sitic: Sibig.F hos Myndighet X

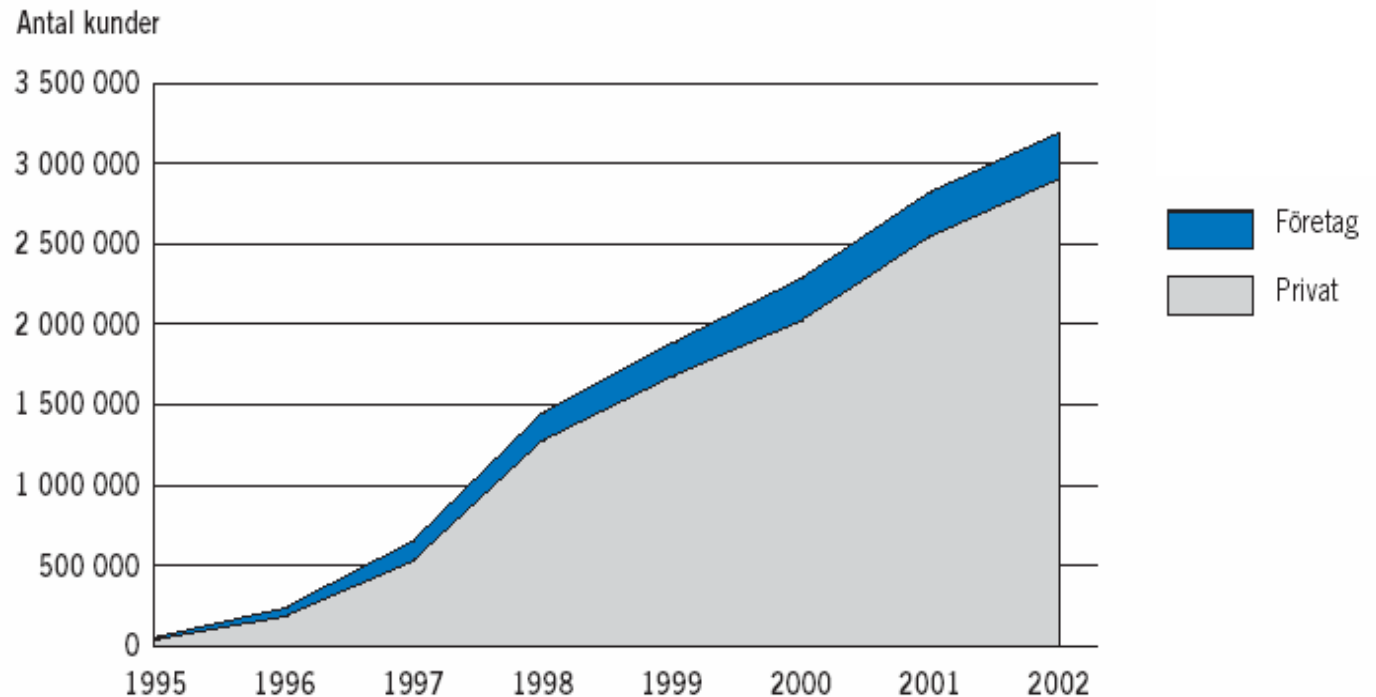


Förklaringar:

CERT/CC: Antal sårbarheter

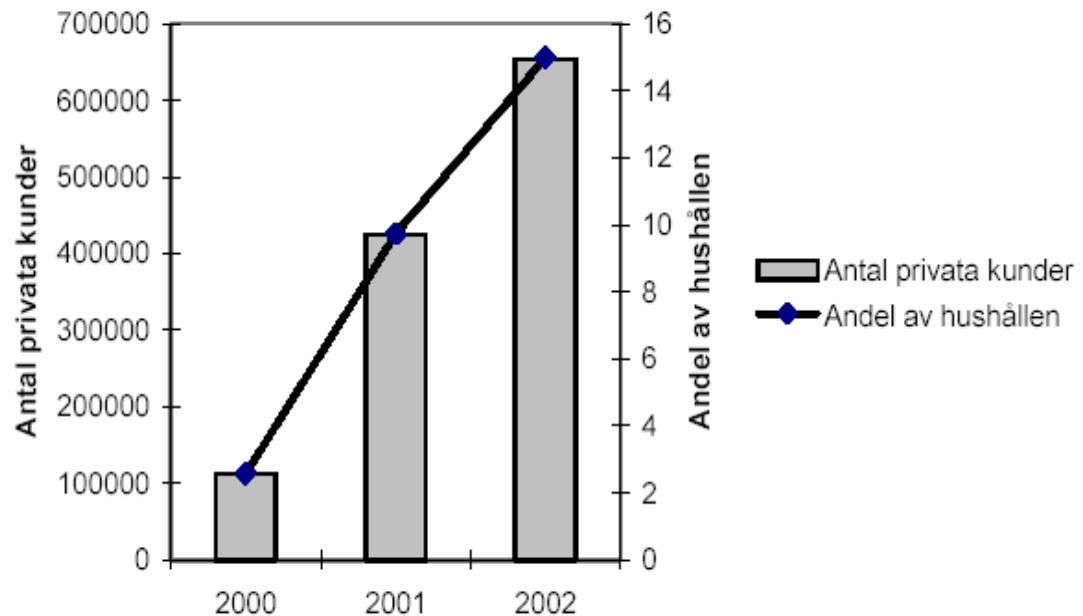


Förklaringar: Internets genomslag



Förklaringar: Bredbandsutbyggnad

Antal privata kunder med Internetaccess via någon form av access med högre överföringskapacitet



Källa: Svensk telemarknad, PTS 2003

Förklaringar: Sobig.F (1/2)

Presscitat:

- Ny Sobig-variant sprids med raketfart
- Vad händer med Sobig.F i helgen?
- Sobig gav under augusti upphov till förluster motsvarande nästan 252 miljarder kronor.
- NN, tekniskt chef på xyz, tror att risken för att det kommer en ny variant av Sobig innan den 10 september är ganska stor.
- Virusmaffia planerar att ta över din dator kl 20.00 ikväll – Så räddar du den.

Förklaringar: Sobig.F (2/2)

Svenska viruslistan augusti 2003:

1. W32/Sobig.F@mm **85,4%** Ny
2. W32/Ganda.A@mm 5,9%
3. W32/Yaha.G@mm 2,0%
4. W32/Bugbear.B@mm 1,8%
5. W32/Mimail.A@mm 1,8%
6. W32/Bugbear.dam@mm 0,8%
7. W32/Klez.H@mm 0,8%
8. W32/Sobig.F.dam 0,7% Ny
9. W32/Yaha.K@mm 0,5%
10. W32/Dumaru.A@mm 0,3% Ny

Källa: Per Hellqvist

Spridningsmekanism:

- Inte genom sårbarhet
- Inte genom ny princip

utan...

”Double click of doom”



POST & TELESTYRELSEN

Förklaringar: Gibe/Swen (1/2)

Presscitat:

- Varning för masken Swen
- Swen är på krigsstigen - Outpost24 höjer varningsnivån.

Osv osv.



Förklaringar: Gibe/Swen (2/2)

MessageLabs 2003-09-23:

1. W32/Swen.A-mm **128000**
2. W32/Klez.H-mm 8000
3. W32/Mimail.A-mm 7000
4. W32/Dumaru.A-mm 4000
5. W32/Sobig.F-mm 2300
6. W32/Yaha.P-mm
7. W32/BugBear.B-mm
8. W32/Sobig.A-mm
9. W32/Klez.E-mm
10. W32/Yaha.E-mm

Spridningsmekanism:

- Inte genom sårbarhet
- Inte genom ny princip

utan...

"Double click of doom"



POST & TELESTYRELSEN

Förklaringar: "Nästa RPC-mask"

Presscitat:

- Hål i Microsoft kan locka ny mask ... lika elak som Blaster...
- Datavärlden varnar för att ett nytt datavirus, värre än Blaster, kan drabba världen inom 14 dagar.
- Förra gången dröjde det tre veckor från det att Microsoft varnade...

Hoten mot internet som viktig samhällsresurs

- Stater nja...
- Kriminella jobbars...
- Hackers jobbars...
- Användare JA!
 - Kategori 1 Använder, kan
 - Kategori 2 Använder inte, kan inte
 - **Kategori 3** **Använder, kan inte**

Hushållens mognadsgrad

Typ av säkerhetsåtgärd	Andel av Internetanvändare med uppringd access	Andel av Internetanvändare med bredbandsaccess
Säkerhetskopior	8 %	10 %
Inloggningsfunktion	16 %	20 %
Brandvägg	13 %	52%
Uppdaterat virusprogram	50 %	67 %

Källa: PTS, 2002

CERT/CC: Ökande attacker mot hemanvändare

- intruders now targeting cable modem/DSL networks
- high concentration of home users
- home systems less likely to be configured securely
- home users less likely to realise they are compromised
- compromised home systems used to launch attacks against other systems
- access to home systems might provide backdoor access to organisations' computers

Hushållens utlämning av personliga uppgifter på internet

Typ av personlig uppgift	Andel av <u>alla</u> Internet-användare	Andel av Internet-användare med uppringd access	Andel av Internet-användare med bredband
Hemadressen	56 %	53 %	65 %
Privat telefonnummer	49 %	46 %	59 %
Privat e-postadress	68 %	65 %	81 %
Eget personnummer	27 %	25 %	33 %
Eget bankkonto/pg-kontonr	7 %	6 %	10 %
Eget konto-/kreditkortsnr	13 %	9 %	22 %

Källa: PTS

Gamla strukturer demonteras

- antalet transaktioner för samtliga betaltjänster hos Posten/Svensk Kassaservice sedan 1998 fallit med i genomsnitt 16 % per år.
- 39 % uppger att de använder internetbank (år 2003)
- Enligt Svenska Bankföreningen fanns vid utgången av 2002 4,4 miljoner internetkunder hos svenska banker

"Call to action", 2002 Australian Computer Crime and Security Survey

- The whole IT security "industry" is responsible for reducing the rate of Australian computer crime
- We need to more effectively communicate security risks and issues, both publicly and privately
- We need to understand IT security as a business risk issue, not a technology issue
- Only by encouraging incident reporting and information sharing will real progress be made

Vägen framåt: Några komponenter

- Media, "framsidan av myntet": Öka medvetandegraden
- PTS:
 - Sitic
 - Regeringsuppdraget "Information till internetanvändare" 2003Q4
- ISP?
- Antivirus- och andra leverantörer?
- Övriga?
- ***Vad har du själv för förslag?***