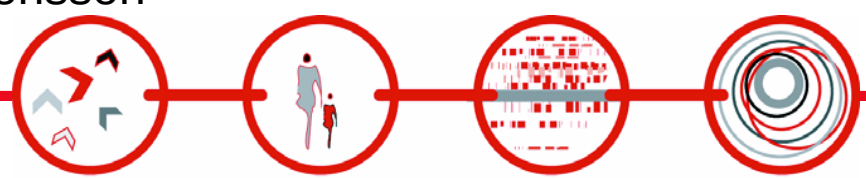
Sveriges IT-incidentcentrum

Orsakssamband

Den bistra verkligheten

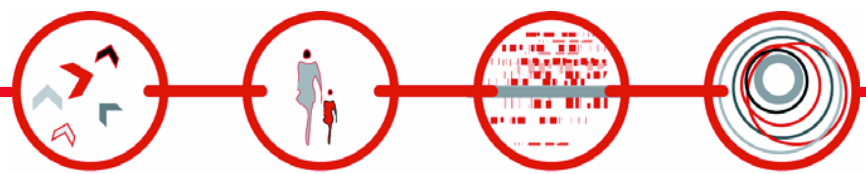
Internetdagarna 2005

Johan Mårtensson



Presentationsstruktur

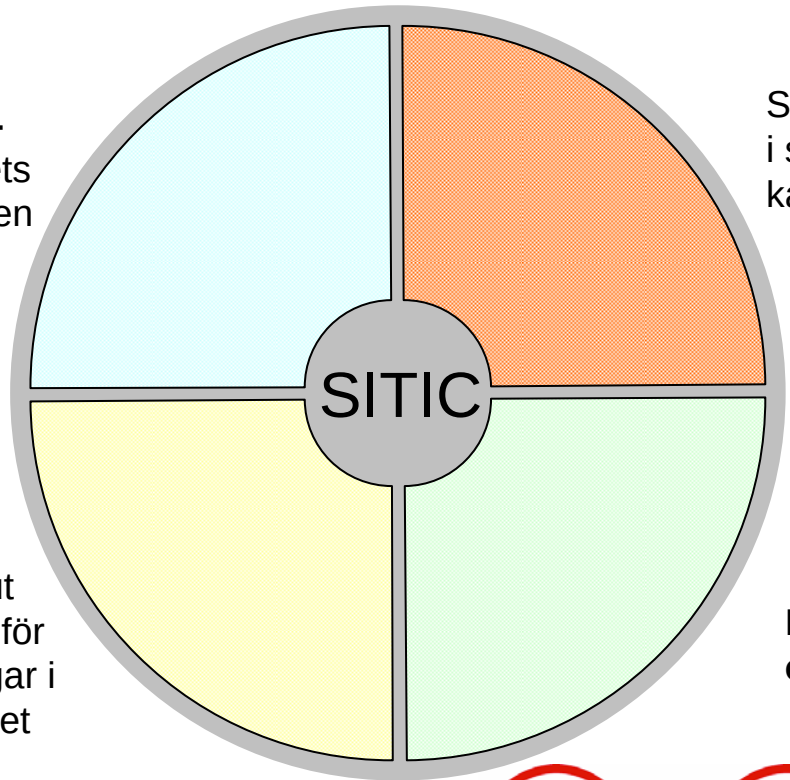
- Spelplanen – vilka ”utgör” internet
- HemPC-reformen – ett skott i foten?
- Verktygen – kunskap, produkter, lagar mm
- Dominerande problem
- Vad händer nu?



PTS uppdrag: Sitic

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

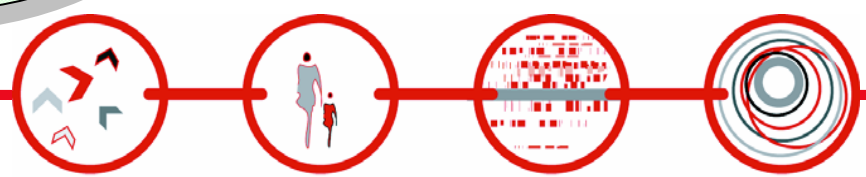
Inrätta ett system för **informationsutbyte om IT-incidenter** mellan samhällets organisationer och funktionen



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

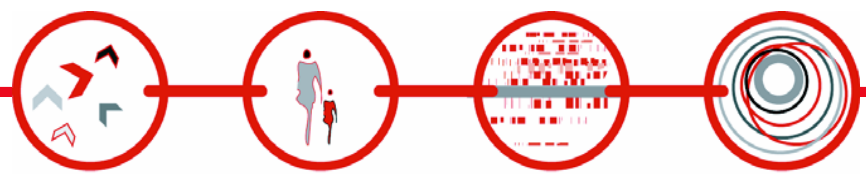
Sammanställa och ge ut **statistik** som underlag för kontinuerliga förbättringar i det förebyggande arbetet

Lämna information och **råd om förebyggande åtgärder**

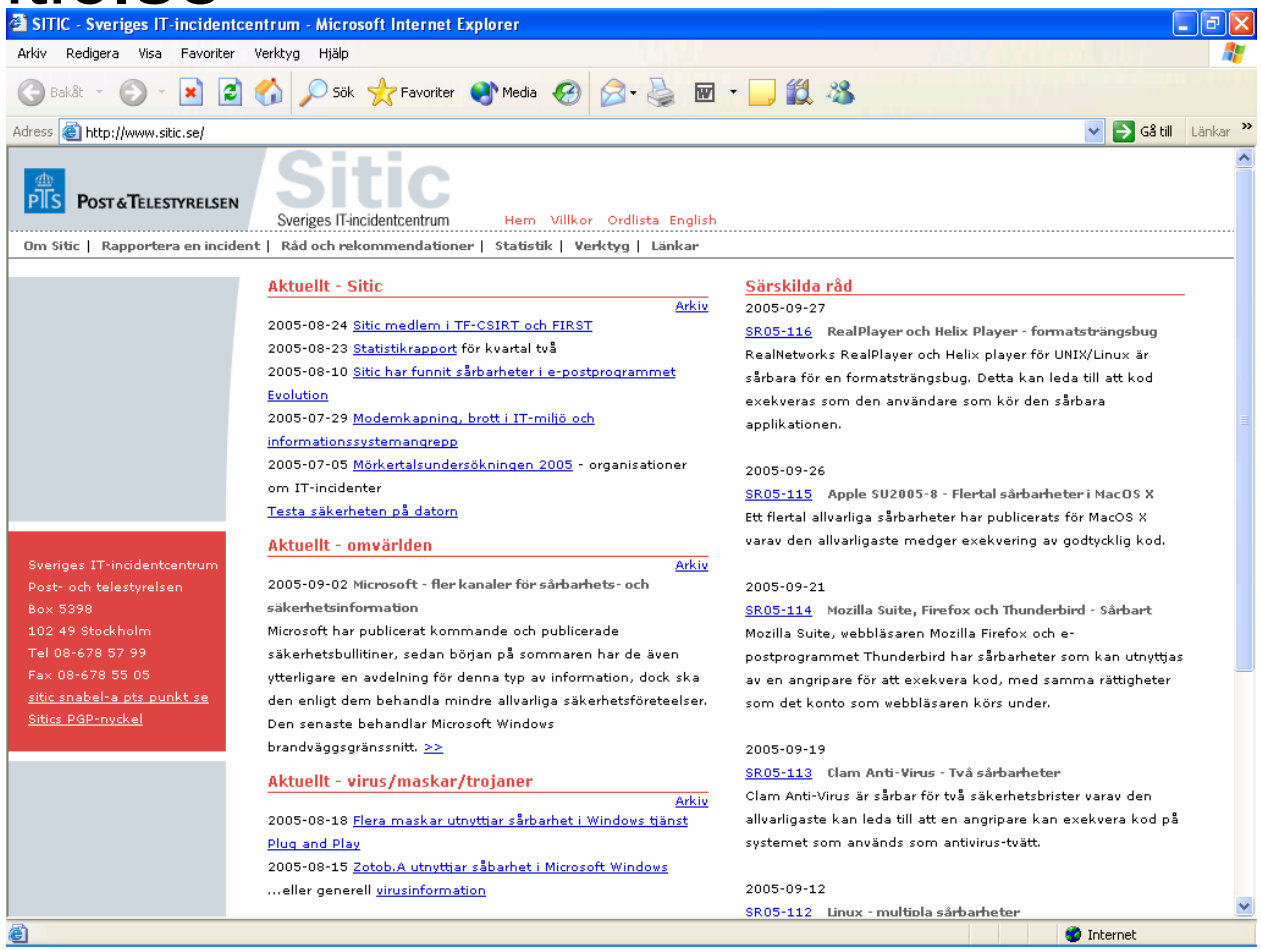


Sitics produkter

- Särskilda Råd
  - Omvärldsbevakning
  - Samarbetande organisationer
  - Egen forskning
- Blixtmeddelanden
- Meddelanden (attackerade sajter)
- Förebyggande Råd
- Statistikrapporter
- Verktyg
- Seminarier och föreläsningar

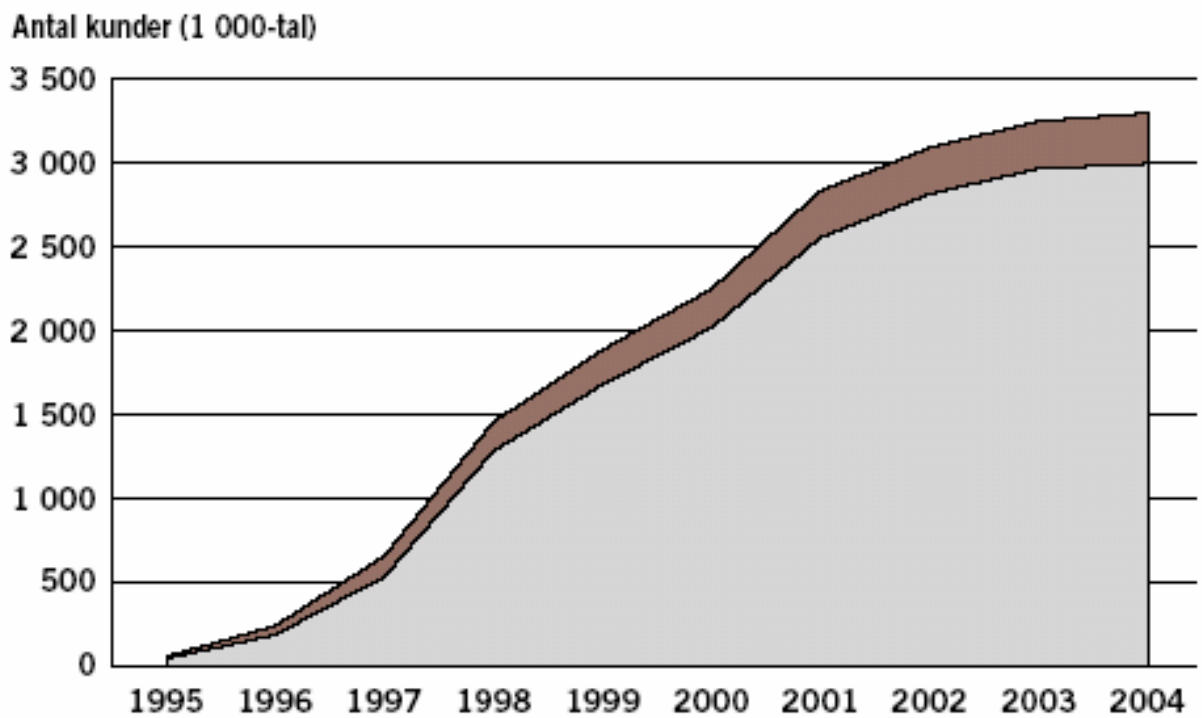


www.sitic.se

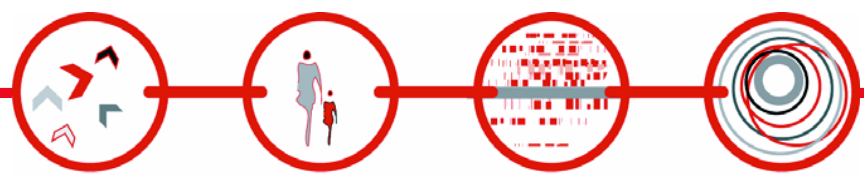

SITIC - Sveriges IT-incidentcentrum - Microsoft Internet Explorer
Arkiv Redigera Visa Favoriter Verktyg Hjälp
Bakåt Sök Favoriter Media
Adress http://www.sitic.se/
Gå till Länkar
Post & Telestyrelsen
Sitic
Sveriges IT-incidentcentrum
Hem Villkor Ordlista English
Om Sitic | Rapportera en incident | Råd och rekommendationer | Statistik | Verktyg | Länkar
Aktuellt - Sitic
Arkiv
2005-08-24 Sitic medlem i TF-CSIRT och FIRST
2005-08-23 Statistikrapport för kvartal två
2005-08-10 Sitic har funnit sårbarheter i e-postprogrammet Evolution
2005-07-29 Modemkapning, brott i IT-miljö och informationssystemangrepp
2005-07-05 Mörkertalsundersökningen 2005 - organisationer om IT-incidenter
Testa säkerheten på datorn
Aktuellt - omvärlden
Arkiv
2005-09-02 Microsoft - fler kanaler för sårbarhets- och säkerhetsinformation
Microsoft har publicerat kommande och publicerade säkerhetsbullitiner, sedan början på sommaren har de även ytterligare en avdelning för denna typ av information, dock ska den enligt dem behandla mindre allvarliga säkerhetsföreteelser. Den senaste behandlar Microsoft Windows brandväggsgränssnitt. >>
Aktuellt - virus/maskar/trojaner
Arkiv
2005-08-18 Flera maskar utnyttjar sårbarhet i Windows tjänst Plug and Play
2005-08-15 Zotob.A utnyttjar sårbarhet i Microsoft Windows
...eller generell virusinformation
Sveriges IT-incidentcentrum
Post- och telestyrelsen
Box 5398
102 49 Stockholm
Tel 08-678 57 99
Fax 08-678 55 05
sitic snabel-a pts punkt se
Sitics PGP-nyckel
Särskilda råd
2005-09-27
SR05-116 RealPlayer och Helix Player - formatsträngsbug
RealNetworks RealPlayer och Helix player för UNIX/Linux är sårbara för en formatsträngsbug. Detta kan leda till att kod exekveras som den användare som kör den sårbara applikationen.
2005-09-26
SR05-115 Apple SU2005-8 - Flertal sårbarheter i MacOS X
Ett flertal allvarliga sårbarheter har publicerats för MacOS X varav den allvarligaste medger exekvering av godtycklig kod.
2005-09-21
SR05-114 Mozilla Suite, Firefox och Thunderbird - Sårbart
Mozilla Suite, webbläsaren Mozilla Firefox och e-postprogrammet Thunderbird har sårbarheter som kan utnyttjas av en angripare för att exekvera kod, med samma rättigheter som det konto som webbläsaren körs under.
2005-09-19
SR05-113 Clam Anti-Virus - Två sårbarheter
Clam Anti-Virus är sårbar för två säkerhetsbrister varav den allvarligaste kan leda till att en angripare kan exekvera kod på systemet som används som antivirus-tvätt.
2005-09-12
SR05-112 Linux - multipla sårbarheter
Internet

Kunder med internetaccess

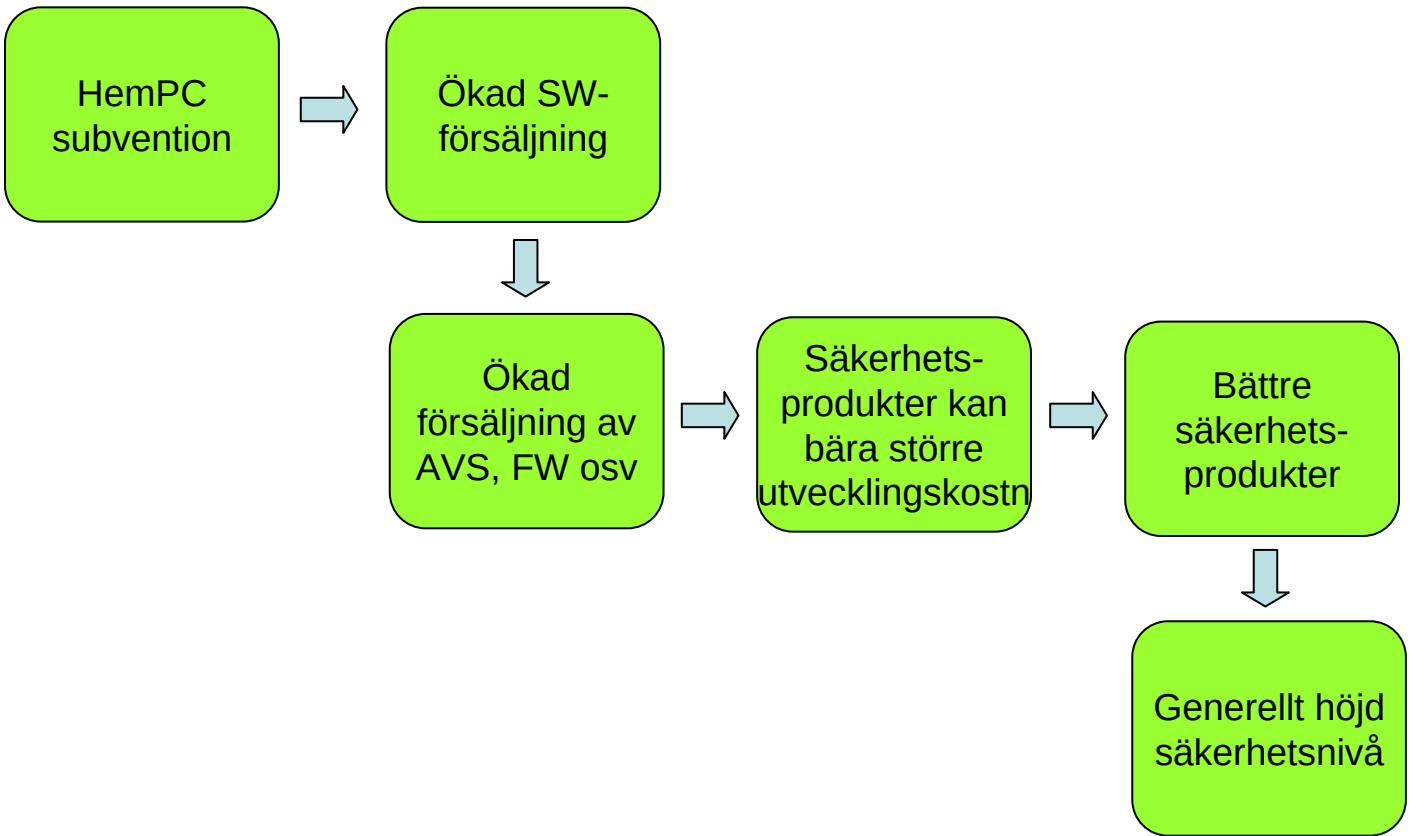
Figur 21
Antalet kunder med Internet-access – företag och privata (december)



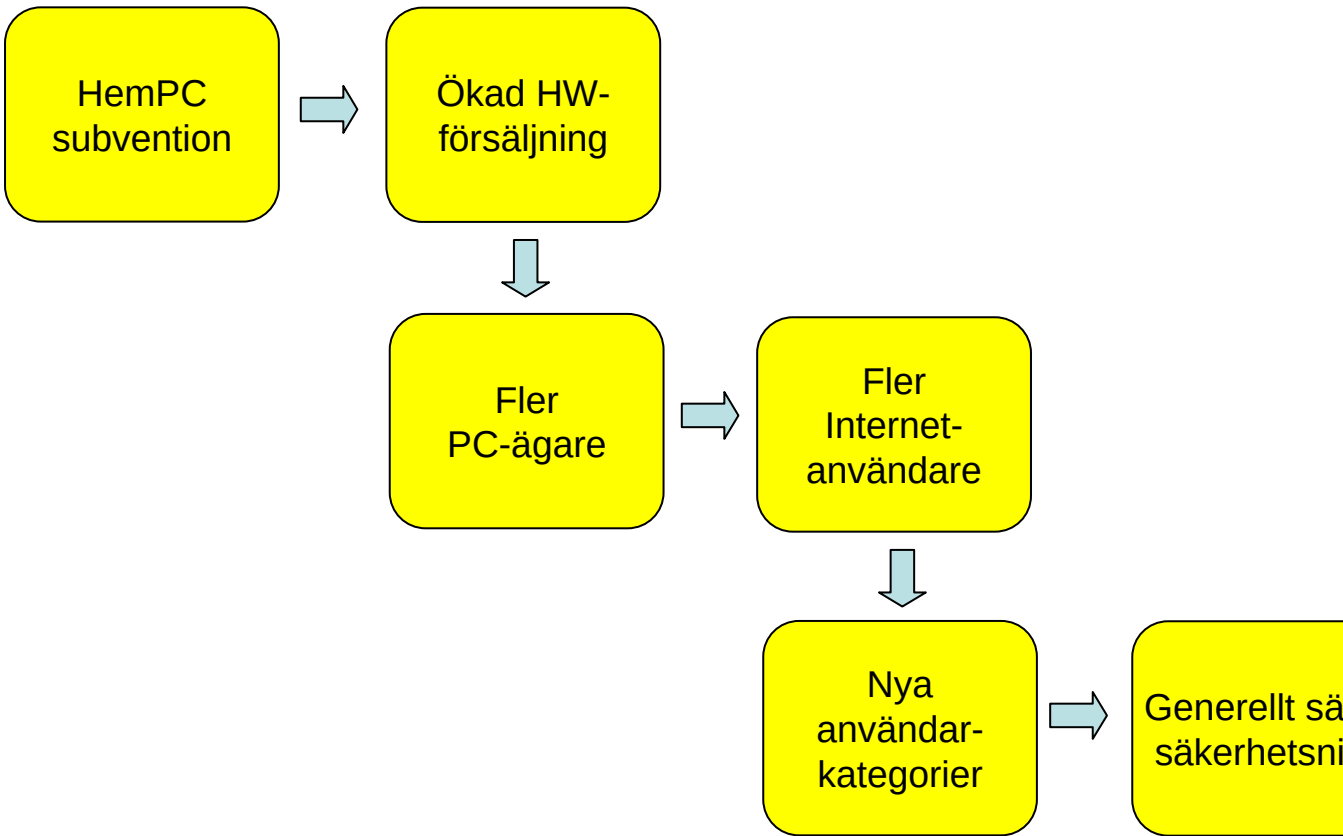
Källa: Svensk telemarknad (PTS 2004)



HemPC vs. säkerhet – positiv kedja

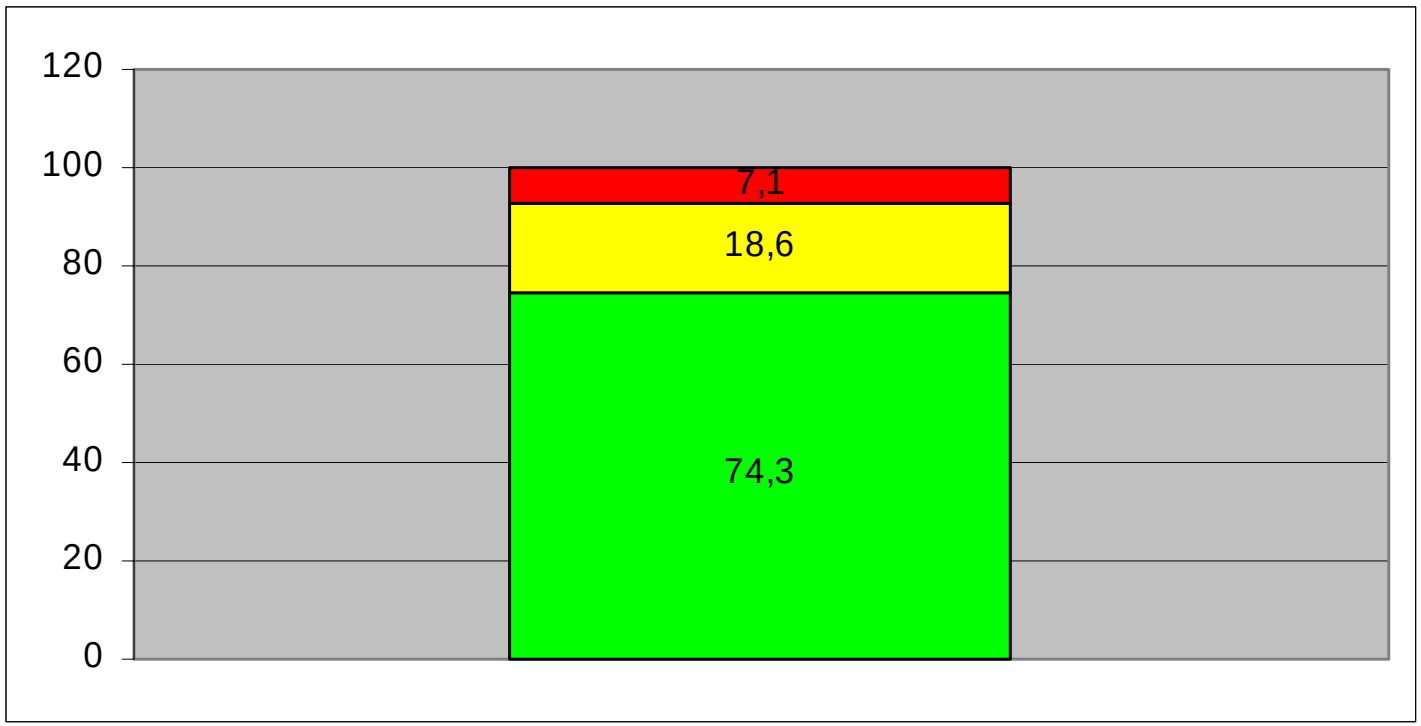


HemPC vs. säkerhet – negativ kedja



www.testadatorn.se

Testutfall



Hemanvändarnas medvetenhet

	2002	2003	2004
Använder brandvägg	23 %	34 %	**47 %**
Har antivirusprogram med uppdaterings-funktion jag nyttjar	53 %	66 %	**78 %**

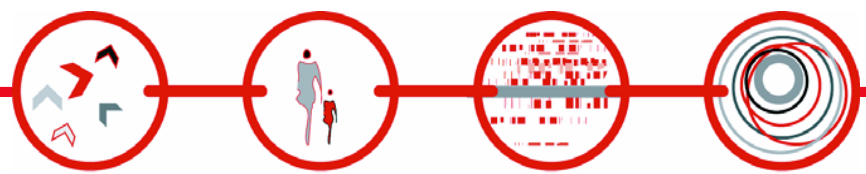
Källa: Så efterfrågar vi elektronisk kommunikation - en individundersökning (PTS 2004)

Hemanvändarens verklighet – granskning av datorer

- 77% trodde sig vara säkra för säkerhetshot
- 2 av 3 saknade kombinationen
  - Uppdaterat antivirusprogram
  - Brandvägg
- 85% hade antivirusprogram installerat
- 72% använde datorn till integritetskritiska aktiviteter (bankärenden, medicinska data osv)

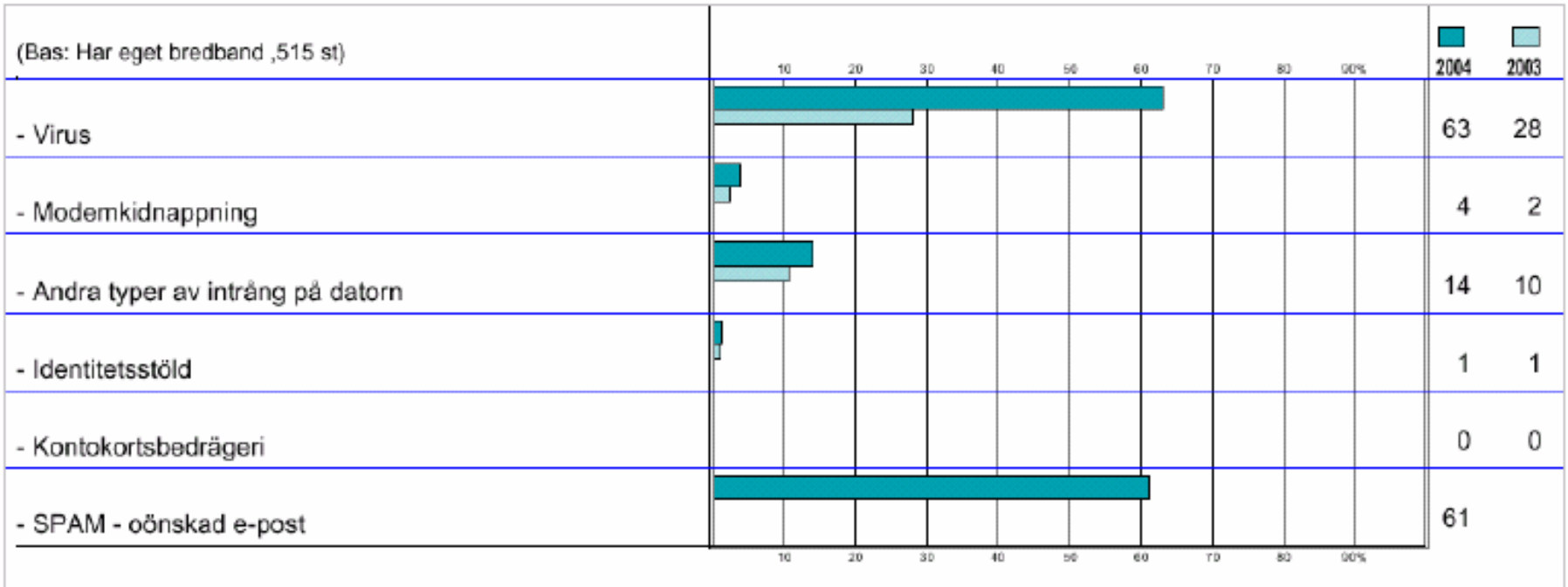
- *80% hade ett flertal spionprogram i datorn*
- *20% hade infektion av skadlig kod i datorn*

Källa: America Online och The National Cyber Security Alliance, Okt 2004



Hemanvändarnas upplevda problem – bredband

Diagram 58: Har du/ditt hushåll någon gång drabbats av följande problem vid Internetuppkoppling från den dator hushållet använder oftast? (Flera svarsalternativ får anges) 2003-2004 (Fråga 61)



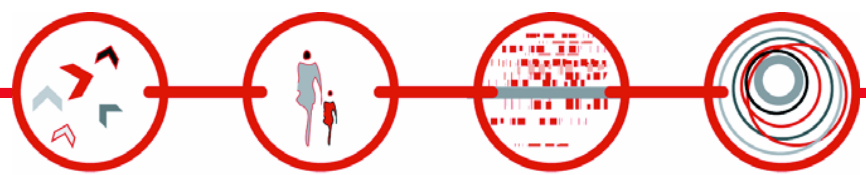
Källa: Så efterfrågar vi elektronisk kommunikation - en individundersökning (PTS 2004)

Hemanvändarnas kostnader

Amerikansk undersökning 2005:

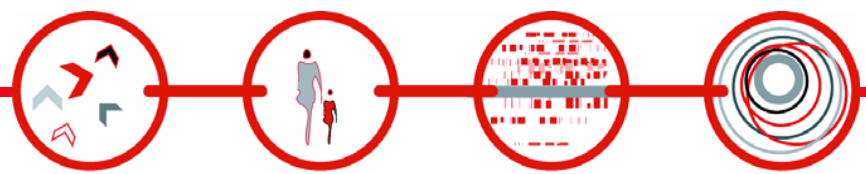
- En tredjedel uppgav att de drabbats av skador (i datorn och / eller finansiellt) av skadlig kod
- Hushållen spenderade 2,6 miljarder dollar på programvara för skydd under 2004
- Hushållen spenderade 9 miljarder dollar på reparationer förorsakade av skadlig kod under 2004

Källa: **State of the Net – Online security 2005** (Consumer Reports 2005)

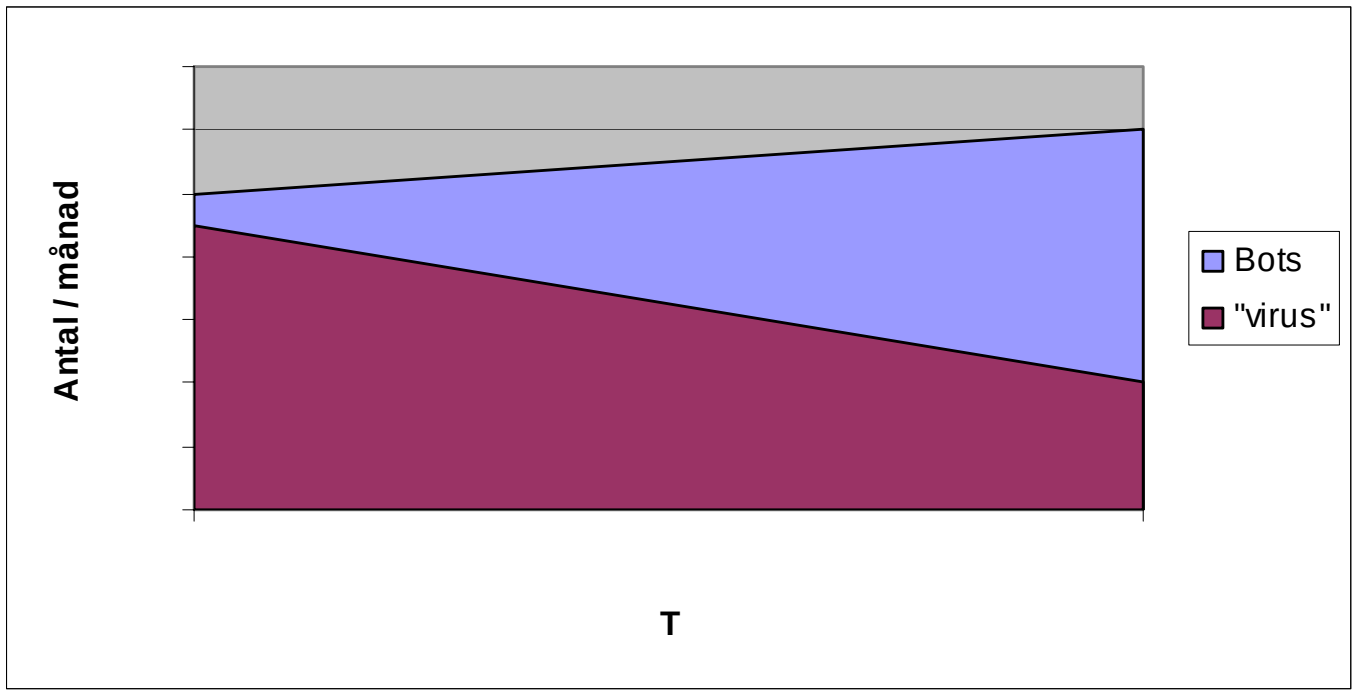


www.pts.se/internetsakerhet

www.surfalugnt.se



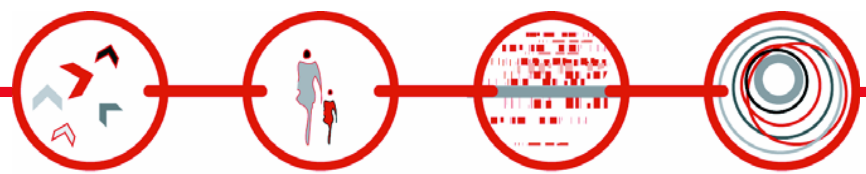
Nya varianter skadlig kod



Mörkertalsundersökningen 2005 (PTS, RPS)

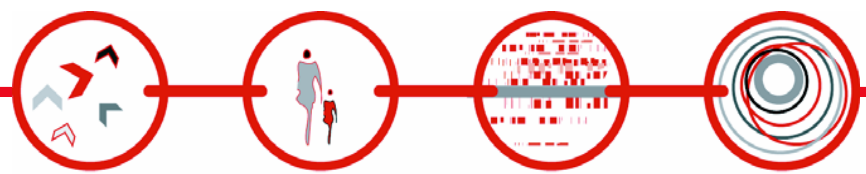
- 45% av de tillfrågade organisationerna hade någon gång drabbats av IT-säkerhetsincidenter
- 28% av organisationerna hade drabbats av IT-säkerhetsincidenter under de närmast föregående 12 månaderna
- Hälften av organisationerna saknade dokumenterade interna rutiner för rapportering av incidenter

Källa: Mörkertalsundersökningen 2005 – Svenska org om IT-säkerhetsincidenter (PTS 2005)



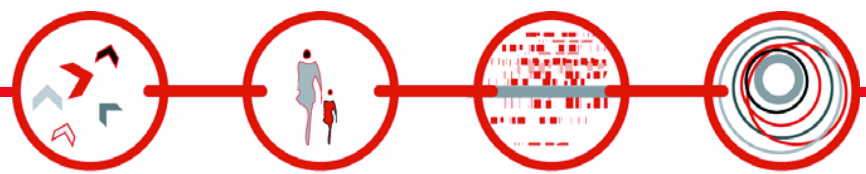
Dominerande problem

- Vi tänker nationellt, men agerar i internationella förlopp
- Internet är en ogästvänlig miljö
- Internet växer så det knakar
  - Noder, tillämpningar
- Kompetensutmaningen – grundkunskaper för nytillkomna
- **Botnets**
  - DoS med utpressning, DoS med politiska motiv, spamutskick, phishing etc
- Spionprogram
  - Integritetsfrågor - Gränserna suddas ut legitimt / skumt



Vad kan stå närmast på tur?

- Fortsatta och förstärkta informationsinsatser
  - Samhälle, ISP, Leverantör
- Tjänstedifferentiering – olika nivåer av hjälp / begränsning för ISP-kunden
- Tillsynsmöjligheter enligt EKOM-lagen version 050701
  - Krav på god funktion och teknisk säkerhet
- Internationella samarbeten för att riva botnets
  - Prio 1 kontrollmaskinerna, prio 2 zombier
- Internationell kompetensöverföring
  - Hjälp till ”nya” länder
- Hype kring skadlig kod för mobila terminaler, mp3-spelare, spelkonsoler etc



Sammanfattning

- Det är kallt därute
- Internet växer så det knakar
- Nya användargrupper som inte får hjälp utgör en systemrisk
- Skickligare och mer målmedvetna krafter ligger bakom många risker
- Många, både privatpersoner och organisationer, vet inte hur de ska hantera incidenter
- Bekämpning av botnets kommer att få prioritet