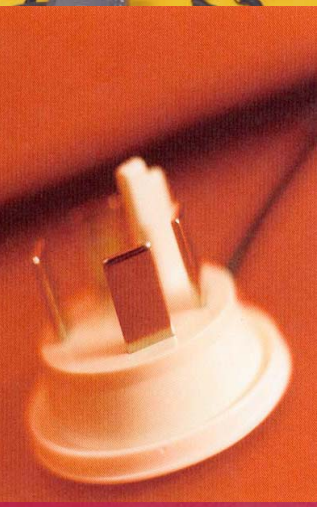


SITIC

Sveriges IT-incidentcentrum

PTS Post & Telestyrelsen

Presentationsstruktur

- Bakgrund
- Uppdrag
- Omgivning
- Intressenter
- Utformning
- Resurser
- Incidentrapportering
- Status

PTS Post & Telestyrelsen

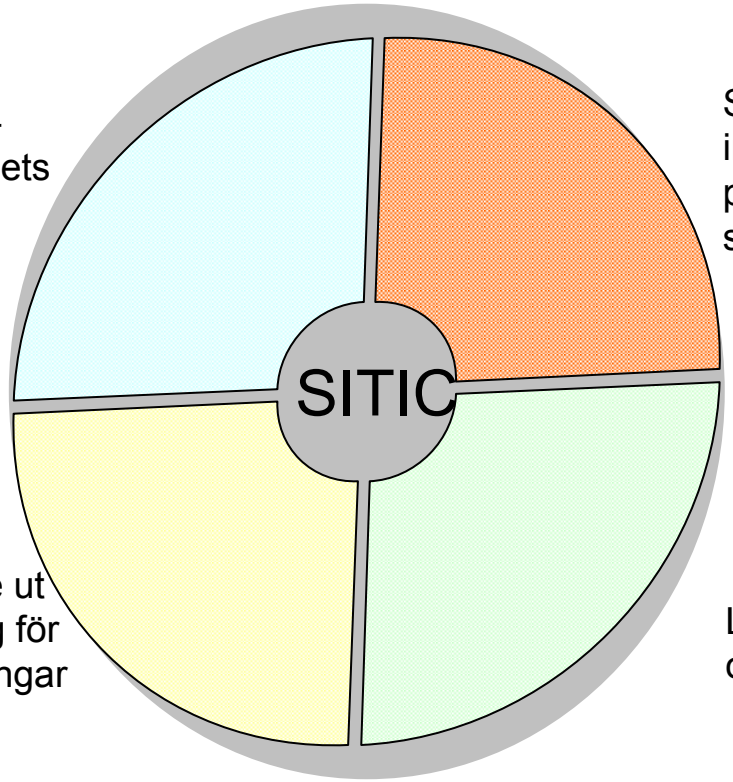
Bakgrund

- PTS rapport ”Förutsättningar för att inrätta en särskild funktion för IT-incidenthantering”, november 2000
- Sårbarhets- och säkerhetsutredningen 2001
- Fortsatt förnyelse av totalförsvaret Prop. 2001/02:10
- Samhällets säkerhet och beredskap Prop. 2001/02:158
- SESIC-projektet avslutat april 2002
- ÖCB:s försöksverksamhet 2000 – 2002 (ca 50 myndigheter)

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

PTS Post & Telestyrelsen

Myndigheter med uppgifter inom IT-säkerhet

- Krisberedskapsmyndigheten (KBM) sammanhållande ansvar för samhällets IT-säkerhet
- En funktion för IT-incidentrapportering (PTS)
- En funktion för teknikkompetens inom IT-säkerhetsområdet (FRA)
- Ett system för evaluering och certifiering (FMV)

Arbetsuppgifter

- Omvärldsbevakning för att upptäcka nya IT-säkerhetsproblem
- Ta emot rapporter om IT-incidenter
- Analys (enskilda incidenter av särskilt intresse, misstänkta säkerhetsproblem)
- Sammanställa och publicera statistik
- Sammanställa och publicera råd (Allmänna, Särskilda)
- Seminarier (egna och andras)

PTS Post & Telestyrelsen

Inledande intervjuer våren 2002

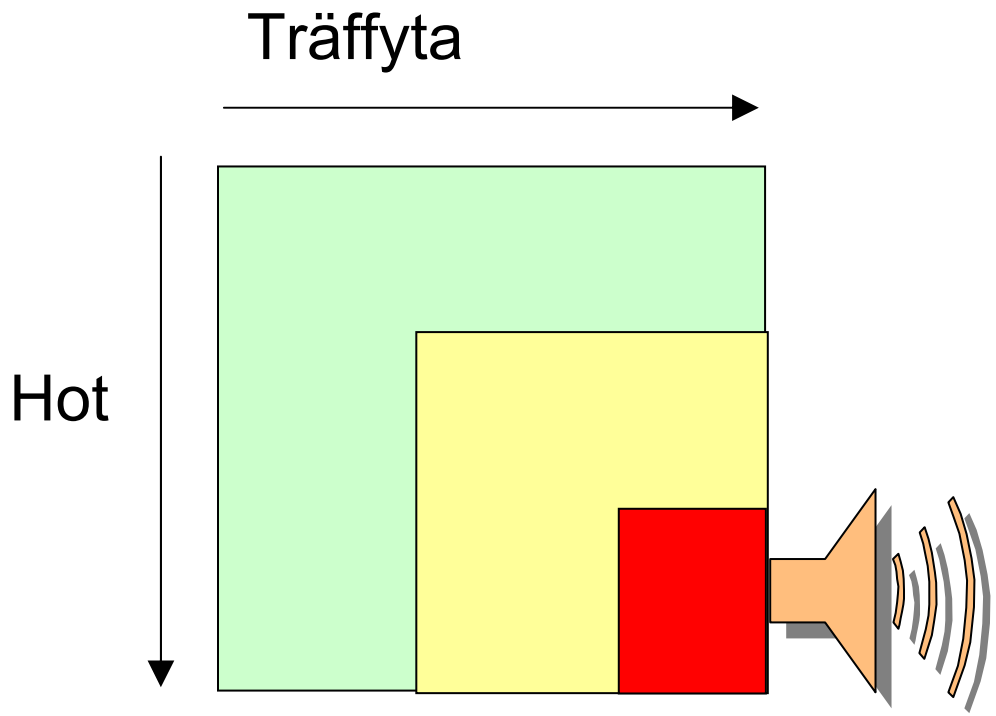
- Råd och utbildning vid uppbyggnad av intern IT-incidentrapportering
- Regelbundna rapporter om IT-incidentläget överlag
- Svenskt forum för IT-incidenter, jmf TF-CSIRT, FIRST
- Sprida ”goda exempel”

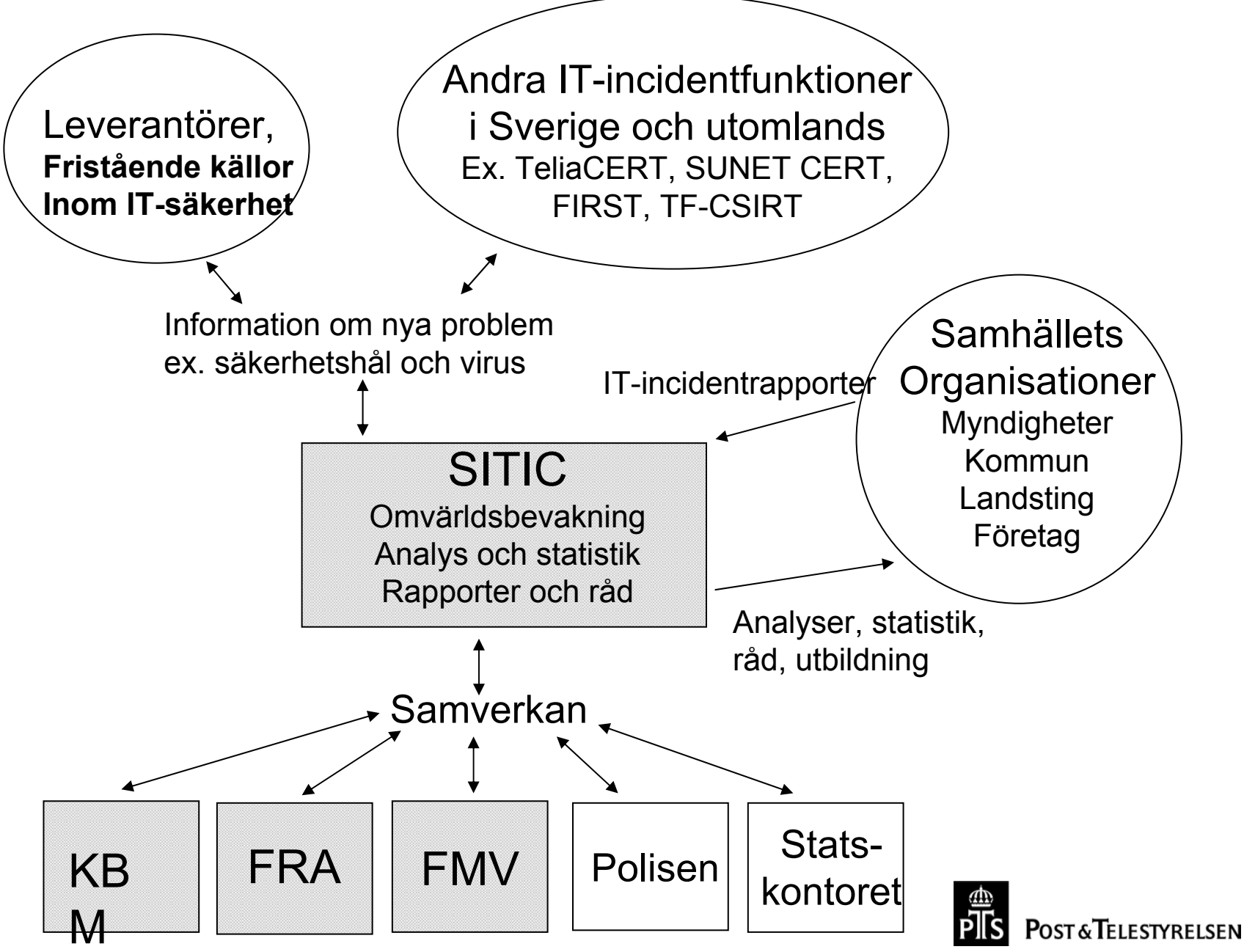
Leverabler

- Allmänna Råd
- Särskilda Råd
- Blixtmeddelanden
- Rapporter med sammanställd statistik
- Öppna och slutna seminarier
- Föreläsningar

PTS Post & Telestyrelsen

Aktivitetsklassning (förenklad)





PTS POST & TELESTYRELSEN

Aktiva myndigheter (urval)

- Riksskatteverket
- Vägverket
- Riksförsäkringsverket
- Polisen
- Statens Strålskyddsinstitut
- Försvarsmakten
- Finansinspektionen
- Jordbruksverket
- Lantmäteriverket
- AMS
- Banverket
- Luftfartsverket
- Svenska kraftnät
- Statens Kärnkraftinspektion
- PTS

PTS Post & Telestyrelsen

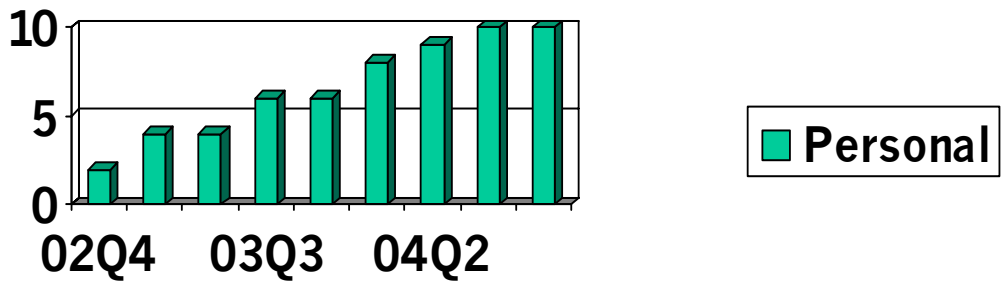
Samverkan med andra CERT:ar

- European Government CERT (statsCERT:arna i Finland, Nederländerna, England, Frankrike, Tyskland och Sverige)
- TF-CSIRT
- FIRST
- Sverige
  - Svenskt CERT Forum
  - SUNET CERT
  - TeliaCERT

Bemanning

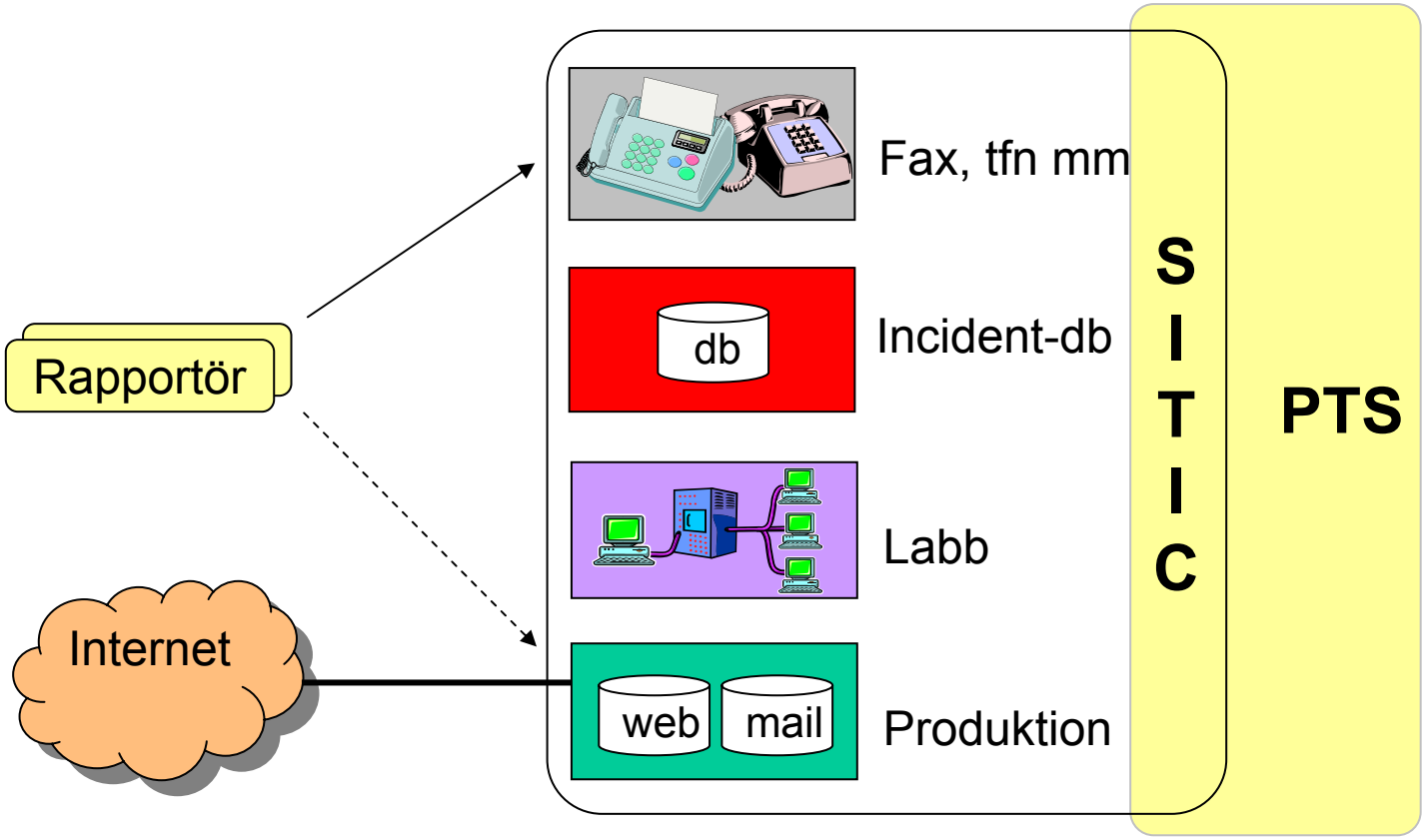
Kompetens

- Teknik: Operativsystem, nätverk, brandvägg, intrångsdetektering, nätövervakning, virusskydd, programmering, drift
- Process: Analys, incidenthantering, standardisering
- Informationssäkerhet, säkerhetsföreskrifter



PTS Post & Telestyrelsen

Fysisk och teknisk miljö



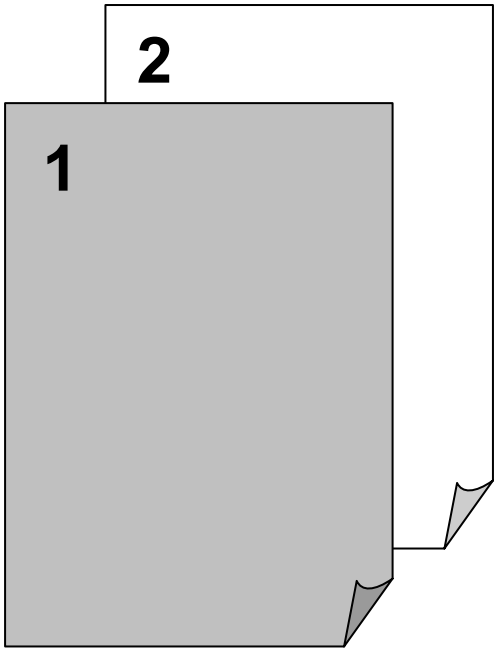
Syftet med Sitic labb

- verifiera varningar angående säkerhetsbrister
- reproducera incidenter för att förstå och finna adekvata åtgärder
- aktivt söka efter säkerhetsbrister i olika produkter
- upprätthålla kompetensen hos Sitics tekniker

Säkerhet

- Labb och produktionsmiljö separerade från PTS övriga system
- Produktionsmiljön har brandvägg och IDS
- Labbet har ingen koppling till externa nätverk
- Rapportering via krypterad fax
- Skalskydd enligt Säkerhetsskyddsförordningen

Incidentrapport - basinformation



Incident

fri text

Auktoritet

definierar avsändande rapportör

Attack

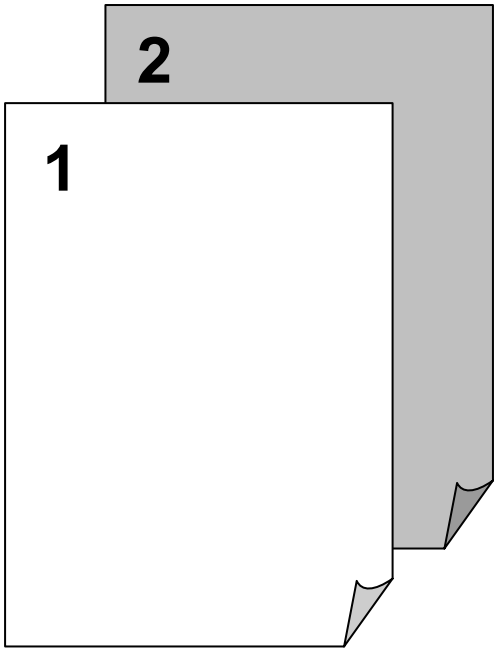
beskriver grunddata för själva incidenten

Metod

beskriver angriparens tillvägagångssätt

PTS Post & Telestyrelsen

Incidentrapport - tilläggsinformation



Metod (fortsättning)

Angripare

beskriver angriparen mer i detalj

Uppteckning

aktivitetslogg från incidenten

Ytterligare Data

Historik

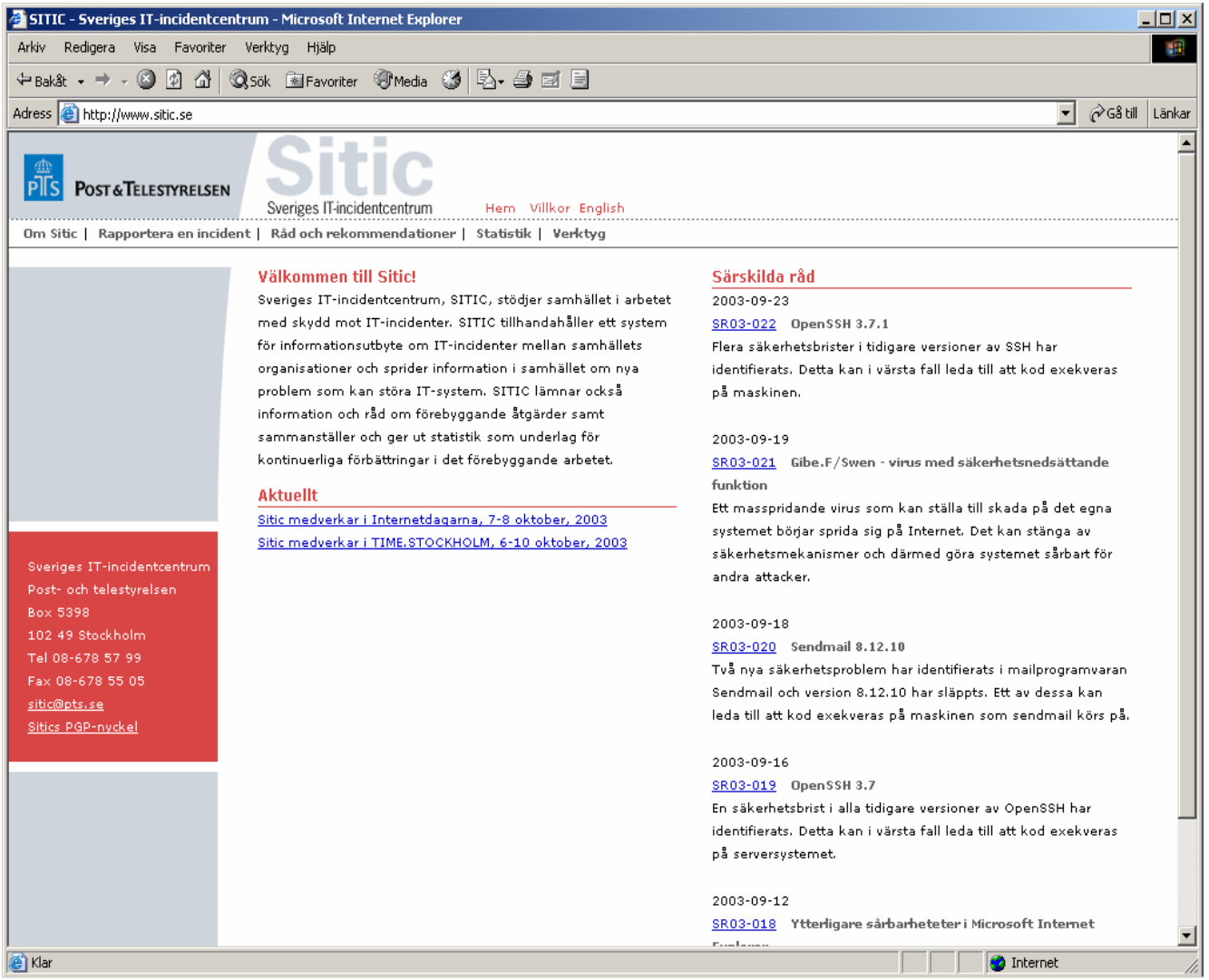
signifikanta händelser under incidenten

Bedömning

rapportörs uppfattning om incidenten

PTS Post & Telestyrelsen

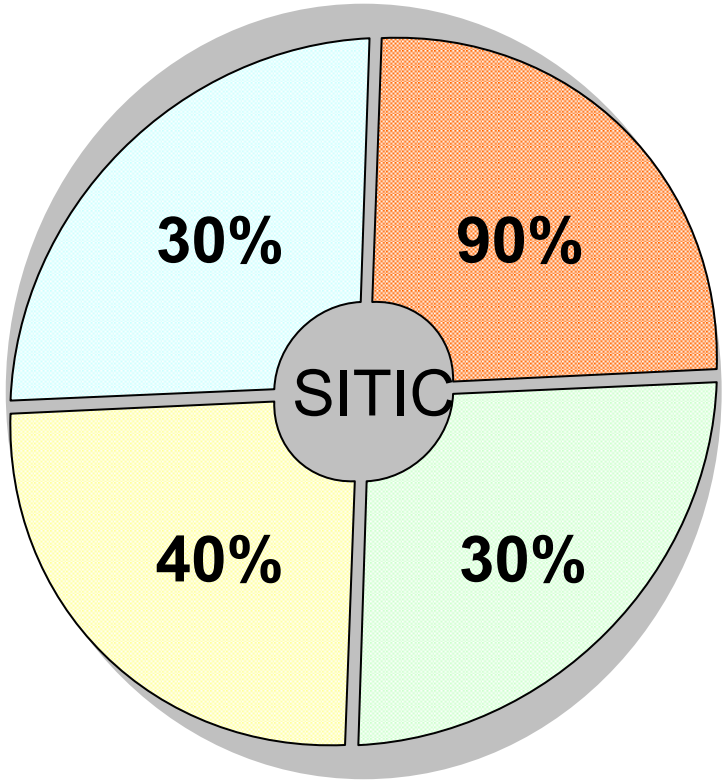
www.sitic.se



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 labmiljö
- Ytterligare rekrytering



PTS Post & Telestyrelsen