

# Kommunikation över gränserna

Sveriges IT-Incidentcentrum levererar konkurrensneutral IT-säkerhet för offentlig sektor och näringsliv

[anders.hansson@sitic.se](mailto:anders.hansson@sitic.se)

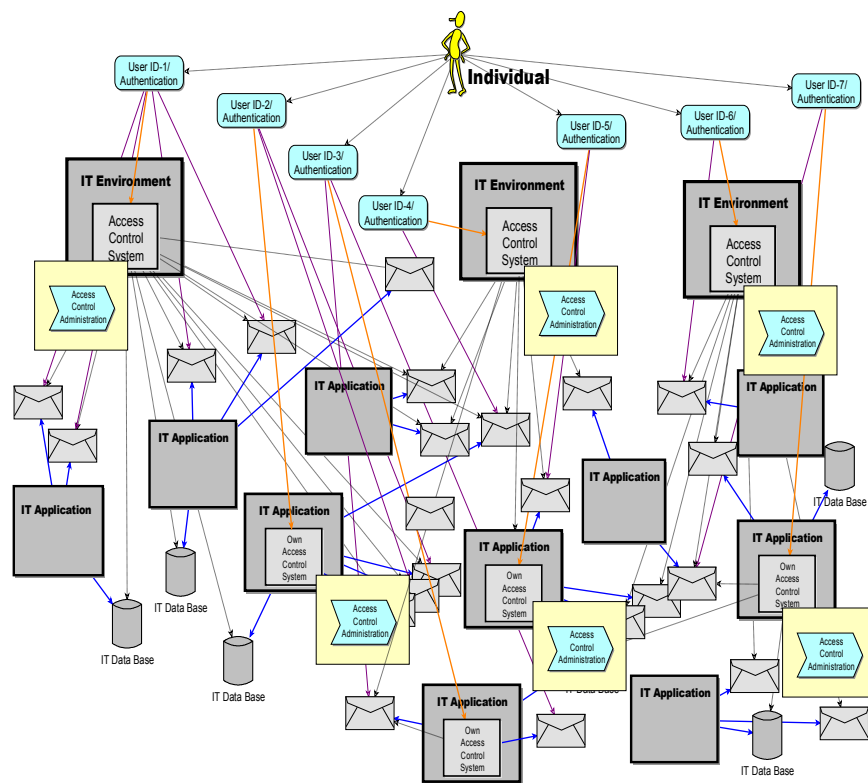
# Instruktionen

- 6 § Post- och telestyrelsen ska svara för att Sverige har en *nationell funktion med uppgift att* stödja samhället i arbetet med att *hantera och förebygga IT-incidenter*. Post- och telestyrelsen ska i detta arbete :
  - agera skyndsamt vid inträffade IT-incidenter genom att sprida information samt *vid behov medverka i samordning av åtgärder* som krävs för att avhjälpa eller lindra effekter av det inträffade.
  - samverka med myndigheter med särskilda uppgifter inom informationssäkerhetsområdet,
  - lämna *råd och stöd avseende förebyggande arbete* till andra statliga myndigheter, kommuner och landsting samt företag och organisationer om nätets säkerhet,
  - vara *Sveriges kontaktpunkt gentemot motsvarande funktioner i andra länder* samt utveckla samarbetet och informationsutbytet med dessa.

# Instruktionen

- 6 § Post- och telestyrelsen ska svara för att Sverige har en *nationell funktion med uppgift att stödja samhället i arbetet med att hantera och förebygga IT-incidenter*. Post- och telestyrelsen ska i detta arbete :
  - agera skyndsamt vid inträffade IT-incidenter genom att sprida information samt *vid behov medverka i samordning av åtgärder* som krävs för att avhjälpa eller lindra effekter av det inträffade.
  - samverka med myndigheter med särskilda uppgifter inom informationssäkerhetsområdet,
  - lämna *råd och stöd avseende förebyggande arbete* till andra statliga myndigheter, kommuner och landsting samt företag och organisationer om nätets säkerhet,
  - vara *Sveriges kontaktpunkt gentemot motsvarande funktioner i andra länder* samt utveckla samarbetet och informationsutbytet med dessa.

# Världen har förändrats



## Exempel på riktade attacker

- Elak kod göms i bilaga, skickas via mail till utvald grupp.
- Ett mail skickas till utvalda med en länk till en server på Internet som har den elaka koden.
- En hemsida (inom en bransch) innehåller elak kod, intresserade surfar dit.
- Belastningsattacker, många förfrågningar görs mot samma hemsida

# Informationssamhället

Sårbarheter

- Pirate Bay 2006
- Muhammed karikatyrer 2006
- Estland 2007
  
- 2009-04-23 - DN:  
Två miljoner datorer drabbade av intrång
  
- 2009-05-10 15:32 - TechWorld Säkerhet  
Stort intrång på amerikanskt toppuniversitet
  
- Fortsättning följer.....





# Vad ger intressanta loggrader?

- Anslutningar
- Autentiseringar
- Transaktioner
- Prestanda / resursanvändning
- Användares kommandohistorik
- Regelverk i brandväggar, IDS/IPS och liknande
- Passersystem
- Samtalslistor (Pizzabutiken?)

# Varför rapportera incidenter?

- Varje enskild rapport ökar möjligheterna att generera relevant statistik och hotbilsrapportering – beslutsunderlag
- Inrapportering kommer andra tillgodo (kan vara först att upptäcka en ny företeelse)

# Varför rapportera incidenter?

- Sitic kan eventuellt associera en inkommen rapport med en eller flera andra (se mönster i hot och angrepp)
- Sitic kan förfoga över (ännu inte) allmänt känd information
- Varje enskild rapport ökar möjligheterna att generera relevanta råd, rekommendationer och andra dokument
- Sitic kan, i särskilt intressanta fall, bidra med spetskompetens, egen såväl som samarbetspartners, i arbetet med analys av händelsen.

# SITIC:s Nationella kanaler

- Samverka med myndigheter med särskilda uppgifter inom informationssäkerhetsområdet
  - MSB – Myndigheten för samhällsskydd och beredskap
  - FRA - Försvarets Radioanstalt
  - FMV- Försvarets Materielverk
  - RKP – Rikskriminalpolisen
  - SÄPO - Säkerhetspolisen
  - FM – Försvarsmakten (FM-CERT)
- Övriga organisationer
  - ISP:er
  - Universitet
  - Media

# Internationell samverkan

- TF-CSIRT (Task Force - Collaboration of Security Incident Response Teams)
- FiRST (Forum of Incident Response and Security Teams)
- IWWN (International Watch and Warning Network)
- ENISA (European Network and Information Security Agency)
- NCF (Nordiskt CERT forum)



# EGC - European Government CERTs

## Syfte med sammanslutningen

- Utveckla överenskomna sätt att hantera
- storskaliga eller regionala incidenter
- Underlätta utbyte av information och teknik
- Dela specialistkunskaper och "best practices"
- Gemensamma projekt

## EGC är en operativ grupp

- "Göra"-fokus, snarare än "prata"
- Sätter ingen nationell policy (förstås)

# Sitics produkter

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

# Sitic, Sveriges IT-incidentcentrum

PTS / SITIC

Box 5398

102 49 Stockholm

Tel 08-678 57 99

Fax 08-678 55 05

[sitic@sitic.se](mailto:sitic@sitic.se)

[www.sitic.se](http://www.sitic.se)