

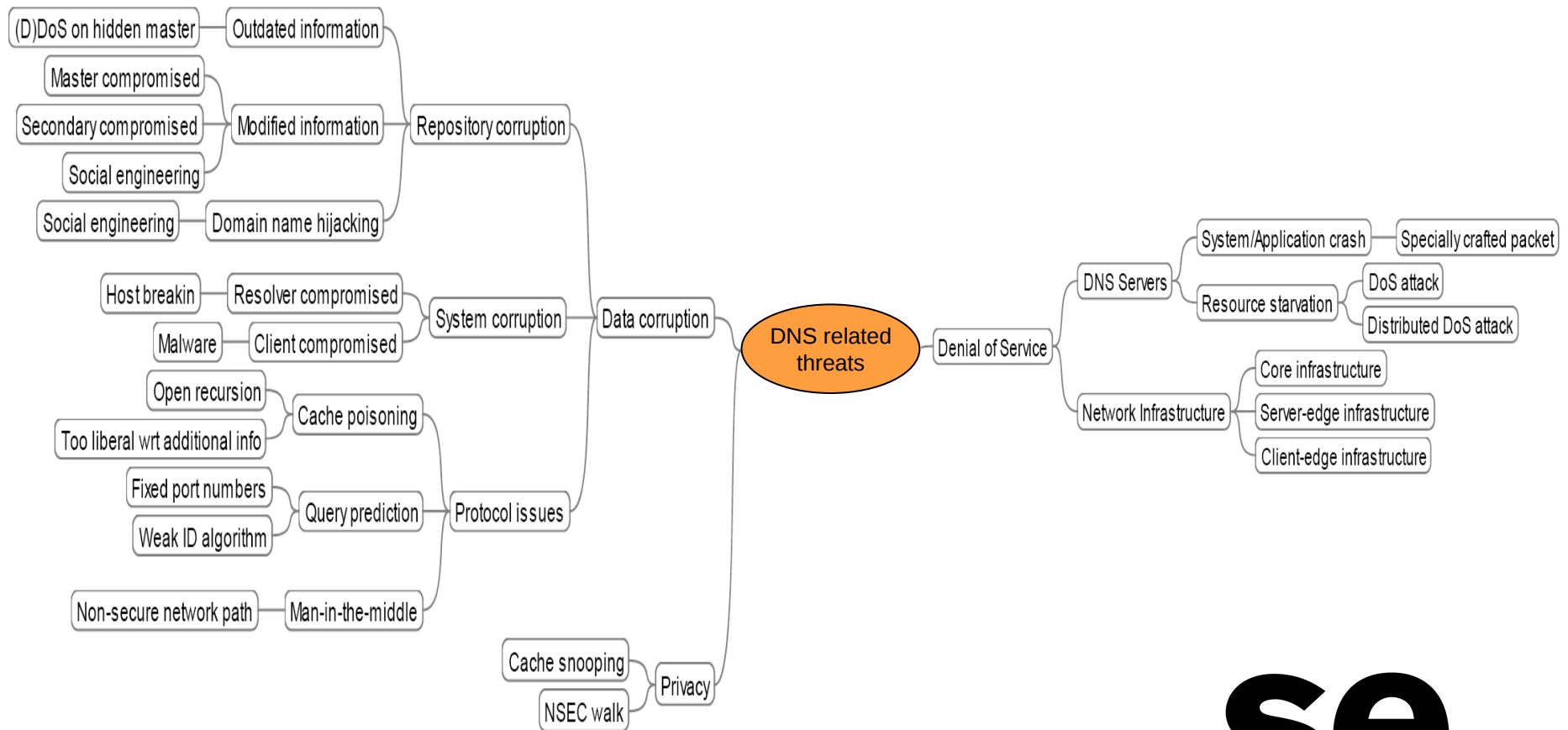


Hälsoläget i .SE 2008

Anne-Marie Eklund Löwinder
kvalitets- och säkerhetschef

.se

Hot mot domännamnssystemet



.se



Undersökning av .SE 2008 – Vad?

- Hur hanterar verksamheter sin DNS?
- Hur hanterar verksamheter sin e-post?
- Hur ansluter verksamheter sin webb till Internet?

.se



Undersökning av .SE 2008 – Vilka?

- 671 domäner, varav 621 klassificerades som samhällsviktiga.
 - Affärsverk och statliga bolag (42)
 - Banker och finansföretag (20)
 - Internetoperatörer (16)
 - Kommuner (289)
 - Landsting (21)
 - Medieföretag (23)
 - Statliga myndigheter inkl. länsstyrelser (260)
- 912 unika namnservrar
- 1870 namnservrar (om man räknar dem per domän).

.se



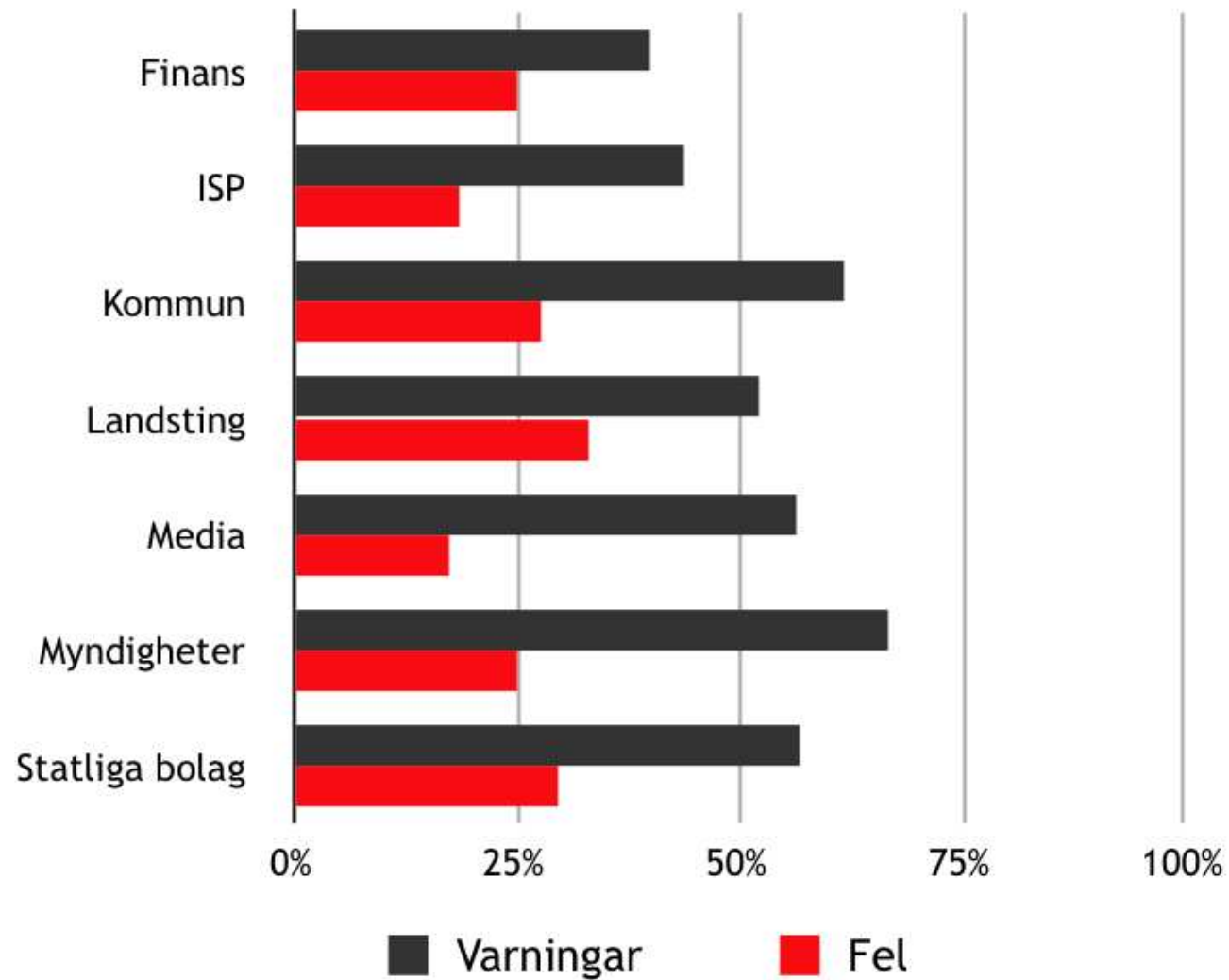
Resultat – tester av DNS

- Av 621 testade domäner hade:
 - 28 procent allvarliga fel. (23 %)
 - 57 procent brister av en karaktär som genererar varning. (64 %)
- Definition av fel och varningar
 - Fel = bör snarast åtgärdas för att verksamheten ska förvissa sig om god tillgänglighet och nåbarhet till DNS och andra resurser.
 - Varningar = är fel som kan påverka driften, men åtgärder bedöms inte vara lika akuta, även om de skulle höja kvaliteten.

.se



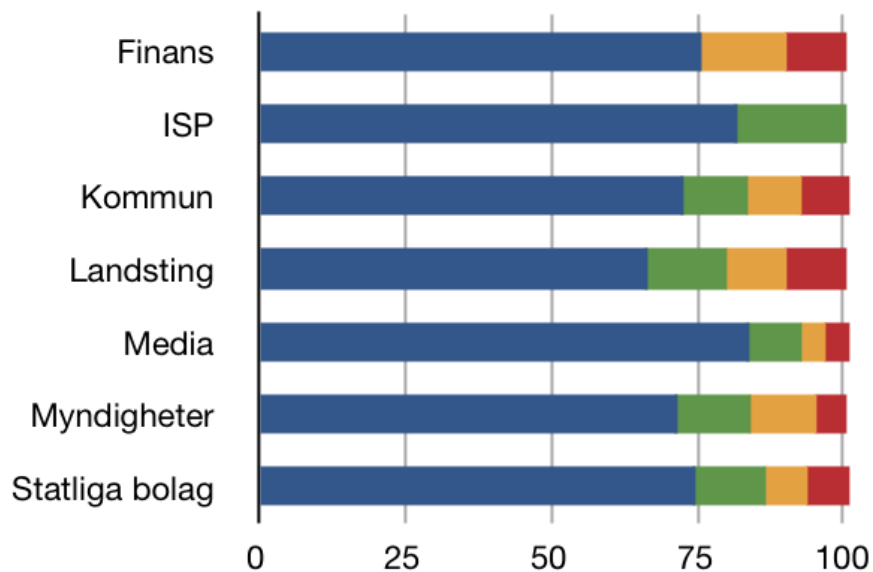
Varningar och fel - 2008



.se

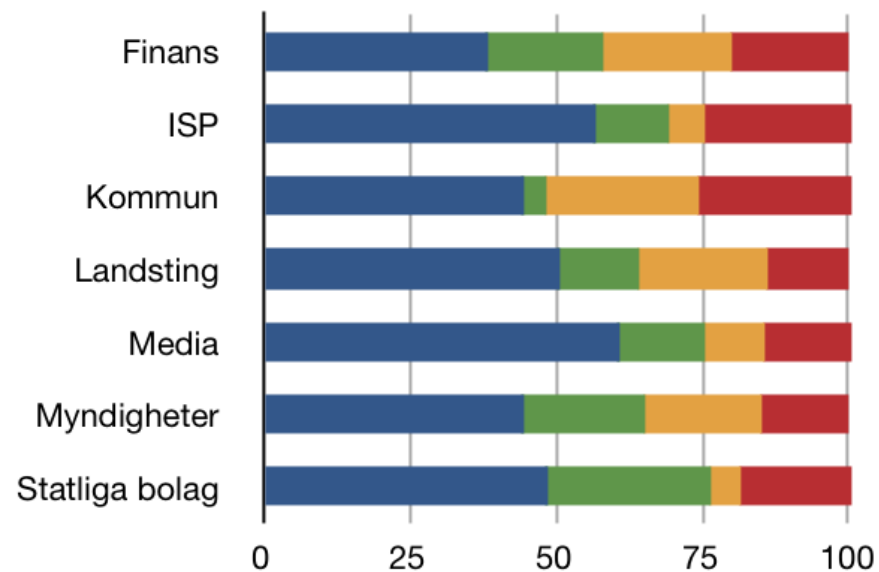


Fel



0 fel 1 fel
2 fel 3 eller fler fel

Varningar



0 varningar 1 varning
2 varningar 3 eller fler varningar

.se



Vanliga fel och brister

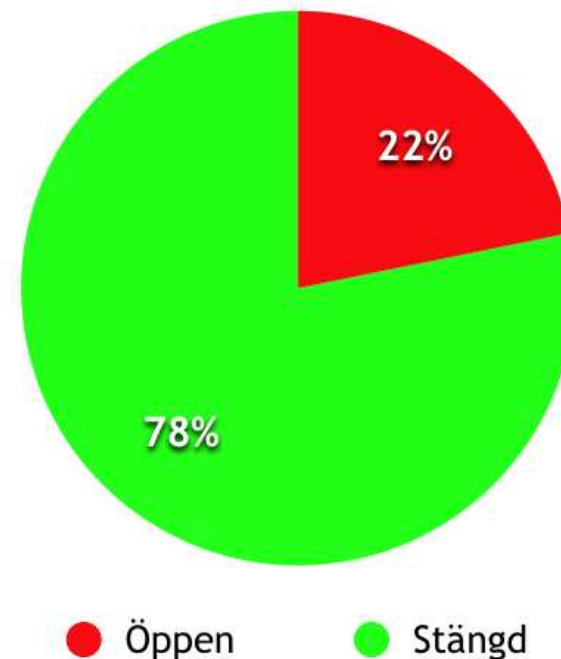
- Namnservern svarade inte på anrop via TCP.
- DNS-servern svarar inte på anrop via UDP.
 - En namnserver som inte svarar på något av dem är förmodligen inte nåbar alls.
- Verksamheten har en icke konsistent namnserveruppsättning.
 - Olika IP-adresser i förälder- och barnzon.
 - Andra namnservrar i förälderzonen än i barnzonen.
- Endast en DNS-server hittades för domänen.
- DNS-servern är rekursiv.
- SOA-serienumret är inte detsamma överallt.

.se

Öppna rekursiva namnservrar

- Har få legitima användningsområden.
- Gör det möjligt för utomstående att utföra tillgänglighetsattacker mot andra via den öppna namnservern.
- Kan missbrukas och bör elimineras.

Rekursiva namnservrar - 2008



.se

DNSSEC

- Säkerställer innehållet i DNS.
- Det enda långsiktiga skyddet mot cache poisoning; t.ex. Kaminskybuggen.
- Endast 8 har infört DNSSEC, 6 kommuner och 2 statliga myndigheter.
- Totalt 891 i hela .SE

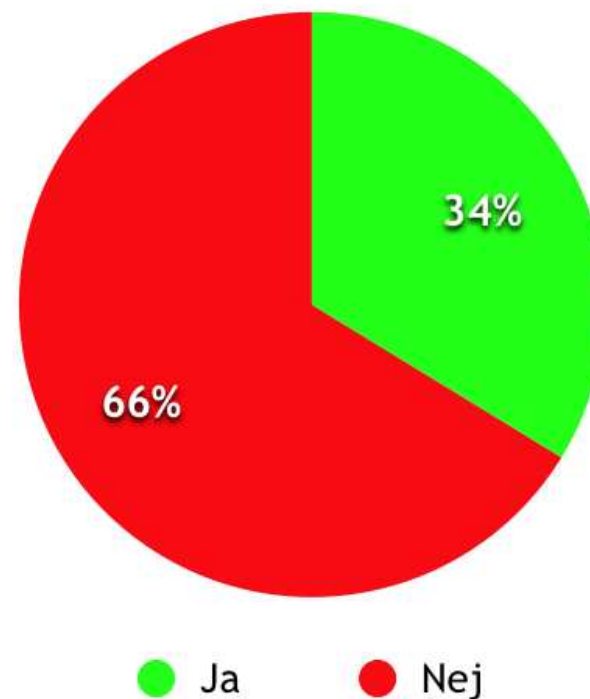


.se

Viktiga parametrar för e-post

- Saknar stöd för transportskydd av e-post: 66 % saknar skydd, oklart om det är aktiverat hos resterande 34.
- Placering: 23 % e-postservrar i utlandet.
- Skydd mot falskt angivande av domännamn i avsändaradressen: 16 %.

E-postservrar med TLS - 2008



.se



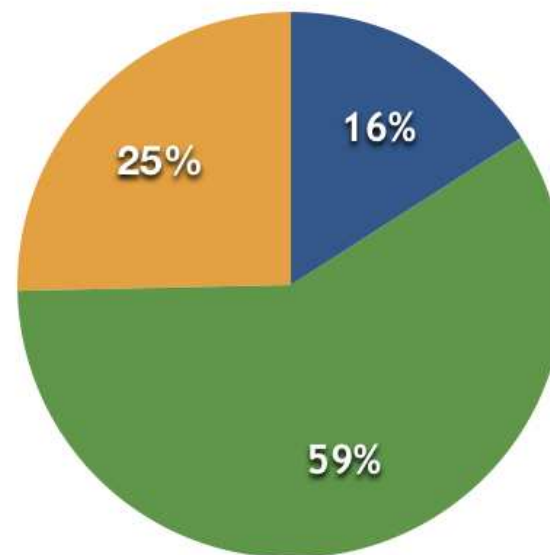
Kategori	Antal servrar	Placerade inom landet (%)
Landsting	41	100
Myndigheter	628	85
ISP	26	81
Bank och försäkring	43	74
Statliga bolag	79	71
Kommuner	484	69
Media	50	68
Affärsverk	8	38

.se

Viktiga parametrar för webb

- Saknar stöd för transportskydd av webb: 25 %, hos de 75 % som har skydd är det i många fall undermåligt infört.
- 722 av 1685 webbservrar skyddas av någon typ av certifikat.
- Endast lite mer än 100 är utfärdade av någon allmänt accepterad CA.

Webbservrar med stöd för TLS - 2008



- TLS med känd CA
- TLS med okänd CA
- Saknar TLS

.se



Behöver vi förbereda oss för attacker?

- Allmänna kommunikationsnät är och förblir en viktig del i samhällets hantering av allvarliga händelser, svåra påfrestningar och beredskapssituationer.
- Nationella och internationella händelser under de senaste åren visar tydligt på vikten av robusta kommunikationer.
- Det är viktigt att utveckla samarbetet mellan myndigheter och i dialog med operatörer och leverantörer, nationellt såväl som internationellt.
- Arbetet med säkerhets- och robusthetshöjande åtgärder innehåller många delar: Skyddsnätet har fler maskor än en.
- Den tekniska och kommersiella utvecklingen skapar många möjligheter men också en del problem.

.se



Råd och rekommendationer

- Anslut kritiska resurser i Sverige till flera operatörer samtidigt, t.ex. med Anycast. Centralt behöver någon bestämma vad som är en kritisk resurs.
- Upprätta en central sekundär DNS-drift för kritiska resurser, t.ex. vid de svenska Internetknutpunkterna.
- Upprätta en gemensam funktion för virustvätt och rensning av skräppost placerad inom landet.
- Utfärda riktlinjer för vad som är acceptabel hantering av skräppost och virus i offentlig förvaltning. Att skicka oskyddad e-post utomlands bör inte vara accepterat.
- Organisera en central CA-funktion för certifikatbaserade tjänster för myndigheter i offentlig förvaltning.
- Ställ krav på offentlig förvaltning om användning av både e-post och webb med käll- och transportskydd.
- Gör tjänster tillgängliga via IPv6.

.se

Tack för mig!



.se