Nåbarhet på nätet

Hälsoläget i .SE 2007

KRISBEREDSKAPS
MYNDIGHETEN

.se

Innehållsförteckning

1 Introduktion

1.1 Detta dokument

Dokumentet är en rapport från ett projekt som .SE genomfört med stöd av Krisberedskapsmyndigheten för att undersöka hur nåbarheten är beskaffad i domännamnssystemet (DNS) i .se-zonen och en del andra viktiga funktioner för domäner i .SE. Dokumentet riktar sig främst till IT-strateger och IT-chefer, men givetvis även till alla andra med ansvar för drift och förvaltning av en verksamhets informationssystem. Den kan förmodligen läsas med behållning även av den mer tekniskt intresserade.

Mer information om innehållet i rapporten kan erhållas från Anne-Marie Eklund Löwinder, kvalitets- och säkerhetschef, .SE. Henne når man på anne-marie.eklund-lowinder@iis.se.

1.2 Förkortningar och ordförklaringar

BCP	Best Common Practice, branschstandard.
DNS	Domain Name System, domännamnssystemet är det system som översätter domännamn (t.ex. iis.se) till IP-adress och som används för kommunikation över IP-nät som t.ex. Internet.
DNS-data	All information om en zon som ingår i DNS.
DNSSEC	Secure DNS. DNSSEC en internationellt standardiserad utökning av DNS som tillför säkrare namnuppslagningar, minskad risk för manipulation av information och förfalskade domännamn. Den grundläggande mekanismen i DNSSEC är kryptografisk teknik som använder digitala signaturer.
SOA	Start of Authority, en pekare på var information om en zon börjar.
TLS/SSL	SSL är en standard för kryptering av bland annat webbtrafik under transport. http över SSL kallas https:Standarden är utvecklad av Ersätts numera av IETF:s öppna standard TLS.
zon	En delmängd av DNS. utpekad från den överliggande nivån i domännamnsträdet.
zonfil	En datafil där alla data om en zon finns lagrade.

2 Sammanfattning

En av fördelarna med datorer är att de ofta döljer komplexa interaktioner så att vi människor slipper veta allt som pågår ”under huven”. En nackdel med detta är att det leder till att de som hanterar information idag i allmänhet har en vag uppfattning om vad som krävs för att hålla en hög kvalitet på t.ex. domännamnssystemet (DNS) för de egna domänerna och därigenom sannolikt också har brister när det gäller drift och operativt ansvar.

.SE har med stöd av Krisberedskapsmyndigheten drivit detta projekt där vi har undersökt i första hand DNS-kvalitet. När vi ändå har varit igång och kört tester på DNS har vi också passat på att titta på några ytterligare - som vi anser viktiga - parametrar för e-post och webb. Undersökningen är genomförd under augusti och september 2007.

Testerna har omfattat totalt 828 domäner och 1043 olika namnservrar. Av 828 testade domäner hade 23 % allvarliga fel och 64 % brister av en karaktär som genererar varning av testverktyget. Resultaten tyder på att många verksamheter har allvarliga brister i den interna DNS-hanteringen såväl som brister i hanteringen av säkerhet för elektronisk post och webb.

Under utredningen har vi bl.a. tagit reda på fakta för följande kontrollpunkter:

- Hur hanterar verksamheten sitt eget DNS? Vem har hand om DNS för verksamheten, hur är det uppsatt (i relation till vad som är att betrakta som branschstandard eller Best Common Practice, BCP), vilka programvaror används, vad är de största synderna, vilka är de värsta syndarna?

- Hur hanterar verksamheten sin e-post? Står servrarna i eller utanför Sverige, vem är tjänsteleverantör, accepteras TLS/SSL (transportskydd), använder de SPF (en teknik att minska mängden skräppost)?

- Hur ansluter verksamheten sin webb till Internet? Var står servrarna, vilken serverprogramvara används, använder de webbcertifikat, har de stöd för TLS/SSL (transportskydd).

Undersökningen har omfattat statliga myndigheter, affärsdrivande verk och statliga bolag; Internetoperatörer, banker och finansbolag, medieföretag, landsting, länsstyrelser, kommuner samt ett antal av de största börsnoterade bolagen i Sverige, alltså totalt 828 domäner.

Undersökningen har varit helt automatiserad och testerna har omfattat tester av förekomsten av de allra vanligaste fel och brister som vi förknippar med DNS-drift, e-post och webbhantering.

3 Om projektet

Stiftelsen för Internetinfrastruktur (.SE) ansvarar för Internets svenska toppdomän, .SE. Kärnverksamheten är registrering av domännamn samt administration och teknisk drift av det nationella domännamnsregistret under .se. .SE är en oberoende allmännyttig organisation som verkar för en positiv utveckling av Internet i Sverige. Genom .SE:s Internetfond avsätter stiftelsen varje år medel till projekt som på olika sätt bidrar till Internets utveckling och användning.

.SE som har ansvar för drift och administration av alla namnservrar för se-domänen har lång och gedigen erfarenhet av sådant arbete, och har successivt på basis av egna och andras misstag och erfarenheter kommit fram till en Best Common Practice som kan tillämpas även i andra miljöer än på toppdomännivån.

.SE:s lansering av tjänsten SE-DNSSEC för säkrare DNS har bidragit till att ett ökat fokus hamnat på DNS och DNS-drift. Den som har för avsikt att göra sin DNS säkrare genom att köpa tjänsten SE-DNSSEC inser tämligen snabbt att införandet inte låter sig göras med mindre än att de först ser över och strukturerar sin egen DNS-infrastruktur som helhet.

Krisberedskapsmyndigheten, KBM, är en myndighet med uppgift att samordna arbetet med att utveckla krisberedskapen i det svenska samhället. Samhällets krisberedskap bygger på att kommuner, landsting, myndigheter, organisationer och företag tar sitt ansvar och samarbetar med varandra. KBM arbetar också förebyggande med IT-säkerhetsfrågor. Inom ramen för detta arbete genomför KBM IT-säkerhetsanalyser inom samhällsviktiga områden och ger ut råd och rekommendationer för säkring av samhällsviktiga IT-system.

.SE har med stöd av Krisberedskapsmyndigheten finansierat och drivit ett projekt för att kartlägga status för DNS i .SE samt vissa andra viktiga parametrar för e-post och webb. Rapporten har skrivits av Anne-Marie Eklund Löwinder, kvalitets- och säkerhetschef på .SE. Det praktiska genomförandet av testerna och de grafiska presentationerna har utförts på .SE:s uppdrag av Jakob Schlyter, Kirei AB.

Testerna har genomförts på domäner och namnservrar för ett stort antal viktiga verksamheter i samhället som affärsverk och statliga bolag, de största börsnoterade bolagen, banker och finansföretag, Internetoperatörer, kommuner, landsting, mediaföretag och statliga myndigheter inklusive länsstyrelser.

Med dessa tester har vi undersökt hur väl verksamheternas system fungerar i olika avseenden, var de värsta synderna begås och vad det kan få för konsekvenser. Till det knyter vi också rekommendationer om hur vi skulle vilja att det såg ut, mer generellt. Slutligen lämnar vi några råd och rekommendationer om frågeställningar för ansvariga myndigheter som lämpliga att gå vidare med och utreda mer i detalj.

4 DNS-tjänst med kvalitet

Vare sig en verksamhet hanterar sin egen DNS-tjänst eller anlitar någon extern part för driften så är det viktigt att den egna DNS-infrastrukturen ansluter till standard och att den är konstruerad på ett sätt som gör att den tillhandahåller en robust tjänst med god nåbarhet.

I projektet har vi utgått från en definition av vad som är att betrakta som en bra DNS-infrastruktur, en erfarenhetsmässigt uppbyggd branschstandard, eller Best Common Practice (BCP).

Något vi av naturliga skäl inte har kunnat mäta i denna undersökning är om det finns tillräcklig kunskap om domännamnssystemet (DNS) och hur det fungerar i de olika verksamheterna. Det faktum att några av de värsta synderna är relativt vanligt förekommande ger oss emellertid en indikation om att situationen kan behöva bli bättre i det avseendet.

4.1 Vad innebär kvalitet i DNS-tjänsten?

Att ha en DNS-tjänst med kvalitet innebär i korthet att:

- verksamheten har en robust DNS-infrastruktur med god nåbarhet,
- alla inblandade namnservrar svarar på frågor korrekt,
- domäner och servrar är korrekt uppsatta,
- data i domännamnssystemet om enskilda domäner är riktig och äkta,
- verksamheten uppfyller de krav som ställs i relevanta Internet- och andra standarder.

I bilaga 1 redogör vi för de viktigaste punkterna som behöver genomföras för att sammantaget skapa en DNS-infrastruktur med hög kvalitet.

5 Tester och testresultat

De genomförda testerna har omfattat såväl domänernas konfiguration och de namnservrar som svarar på frågor om domänen. De har också omfattat några av som vi bedömer det de allra viktigaste parametrarna för e-post och webb. Vid testerna har en programvara använts som automatiskt kan kontrollera de olika kontrollpunkter som angivits i vår branschstandard för samtliga domäner som ingått i undersökningen, som helhet och per kategori. Programvaran har utöver detta kompletterats med frågor kring hantering av elektronisk post och webb.

5.1 Testobjekt

Testerna har omfattat totalt 828 domäner och 1043 olika namnservrar. Testobjekten har grupperats i kategorier på följande sätt:

- Affärsdrivande verk och statliga bolag (49)
- Börsnoterade bolag (där de inte förekommer i någon annan kategori) (66)
- Banker och finansbolag (22)
- Internetoperatörer (ISP) (18)
- Kommuner (290)
- Landsting (21)
- Mediaföretag (23)
- Statliga myndigheter, inklusive länsstyrelser, exkl. myndigheter under Riksdagen (339)

Av 828 testade domäner hade 23 % allvarliga fel och 64 % brister av en karaktär som genererar varning.

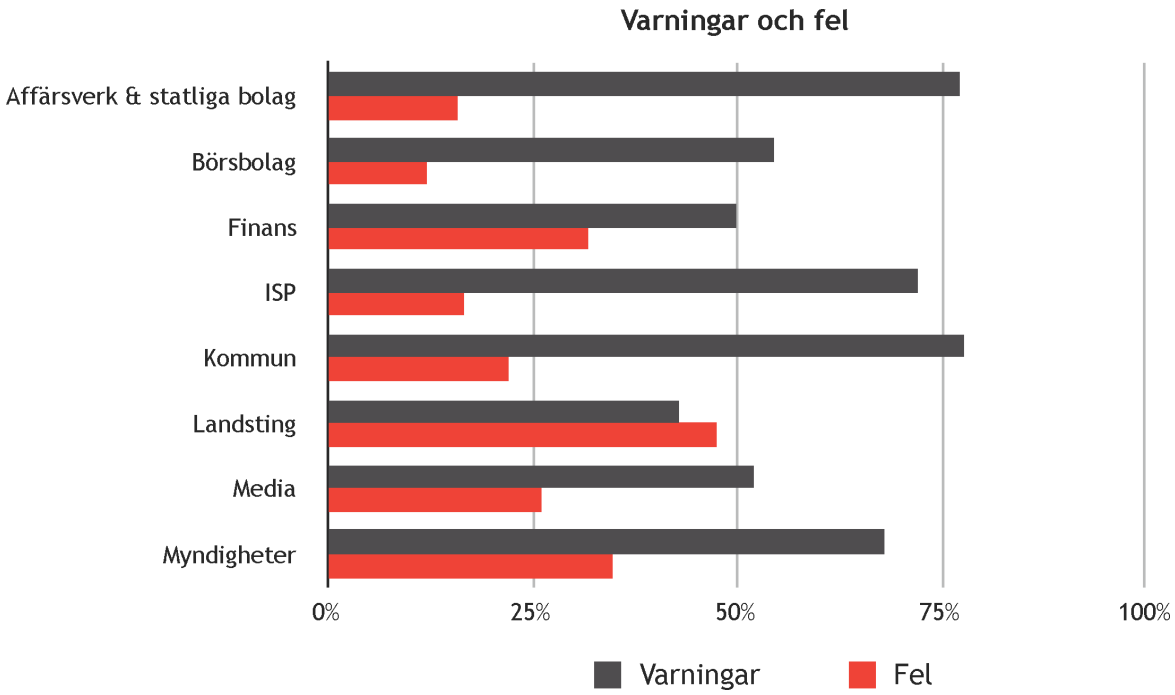
VÄRT ATT VETA

Fel: Det som markeras som fel i undersökningen är sådant som bör åtgärdas för att verksamheten ska kunna förvissa sig om god tillgänglighet och nåbarhet till DNS och andra resurser.

Varningar: Varningar är också fel som kan påverka driften, men åtgärder bedöms inte vara lika akuta, även om de givetvis skulle höja kvaliteten.

5.2 Resultat – tester av DNS

Hur fel och varningar fördelar sig mellan de olika undersökta grupperna framgår av tabellen på nästa sida.



Vi kan av tabellen ovan utläsa att den grupp som har störst andel fel är landstingen. Inom den gruppen är närmare 50 % av alla namnservrar behäftade med någon typ av fel som betraktas som allvarligt. Av den anledningen har vi även grund för en stark misstanke om att tillgängligheten till information och tjänster är långt sämre än vad den skulle behöva vara.

De tester som genomförts har utfallit enligt nedanstående översiktliga redovisning.

- Verksamheten har alla namnservrar stående hos en och samma operatör, 452 domäner.
- Verksamheten har för få namnservrar (NS-poster). Att ha för få namnservrar innebär att man bara har en. Det i sin tur innebär att verksamheten är mycket sårbar om den servern skulle gå sönder eller om förbindelsen till den skulle avbrytas, 21 domäner.
- Verksamheten har namnserver eller domän som inte svarar korrekt på DNS-frågor. Detta beror oftast inte på någon medveten handling från den som driver namnservrar för verksamheten, utan oftast på bristande kunskaper hos operatören eller av den som ansvarar för brandväggslösningen inom organisationen, 180 domäner.
- Verksamheten har en inkonsistent namnserveruppsättning (NS). De namnservrar som listats med NS-poster i en delegerad zon skiljer sig från den information som ligger i DNS i den överliggande zonen, och därmed kan namnservrarna inte svara auktoritativt och korrekt för domänen. Om informationen inte är enhetlig så påverkar det tillgängligheten för domänen negativt och tyder på brister i den interna DNS-hanteringen, 93 domäner.
- Verksamheten har felaktig (s.k. "lam") delegering. Det innebär att domänen pekar ut en namnserver som inte har någon information om denna domän. Det innebär att bland 3

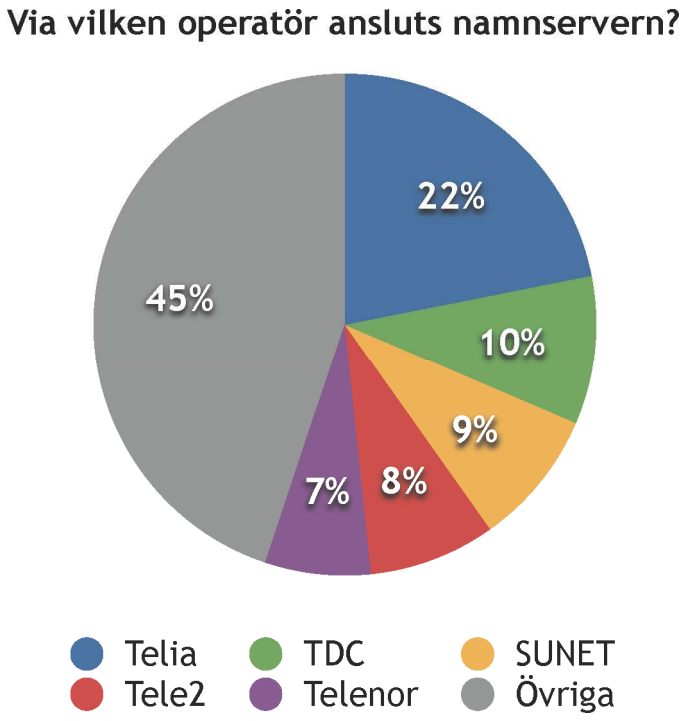
namnservrar så kanske bara 2 svarar på frågor. Det ger bristande tillgänglighet till de egna tjänsterna, och det tyder på allvarliga brister i den interna DNS-hanteringen, 90 domäner.

- Verksamheten har namnserver som annonseras som nåbara med IPv6 men som i realiteten inte är det. Om någon annonserar att man har namnserver som ska vara nåbar över IPv6 och inte har det så innebär det att den som frågar inte kommer att få något svar. Det ger bristande tillgänglighet och det tyder på brister i den interna DNS-hanteringen, 62 domäner.

- Verksamhetens domännamnssystem saknar stöd för stora IP-paket i DNS (Extended DNS eller EDNS). Den domän vars namnservrar saknar stöd för EDNS har med stor sannolikhet en alltför åldersstigen programvara. Avsaknad av stöd för EDNS innebär problem vid införandet av nya funktioner i domännamnssystemet som de facto kräver hantering av längre paket, t.ex. säker DNS (DNSSEC), 42 namnservrar.

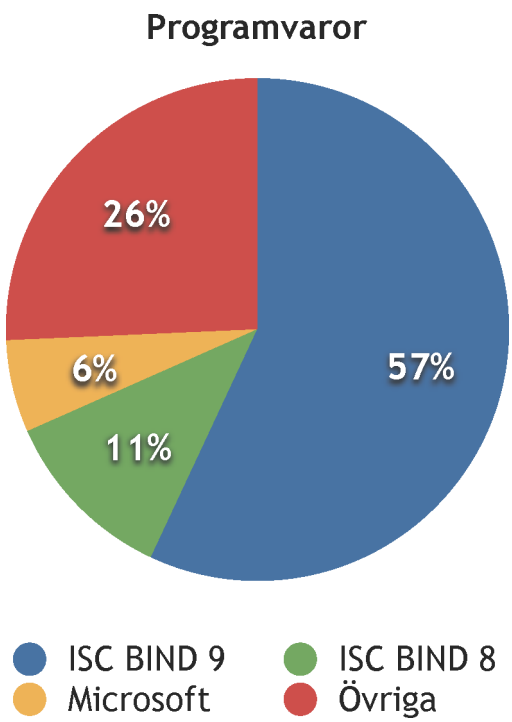
5.2.1 Anslutning av namnserver till Internet

Vi kan konstatera att det finns en relativt god spridning bland operatörer när det gäller anslutning av namnservrar. Ingen operatör dominerar marknaden i någon större omfattning. Skissen nedan visar alltså inte vem som driver namnserver för domänen, utan enbart via vilken operatör namnservern är ansluten till Internet.



5.2.2 DNS-programvaror

Det är ett fåtal olika DNS-programvaror som totalt dominerar marknaden. Allra vanligast är ISC (Internet Systems Consortium) BIND i några olika versioner, men även Microsoft Windows DNS förekommer. Följande figur visar den procentuella fördelningen av de programvaror används för DNS i de testade domänerna och dess namnservrar.

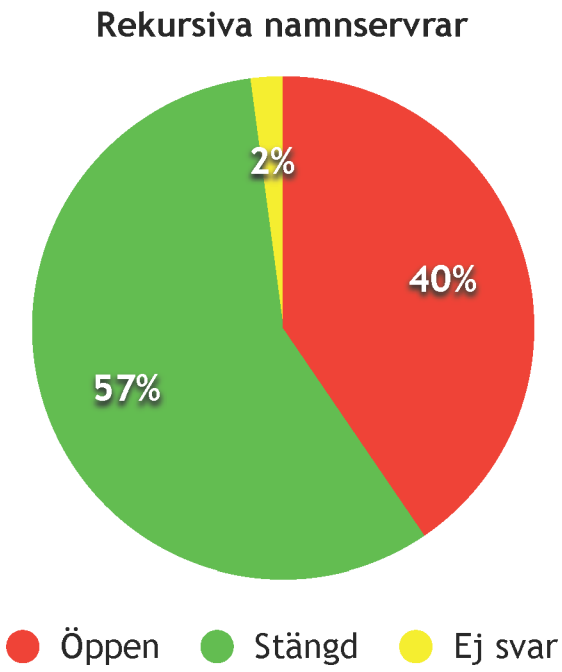


Så mycket som 11 % av de undersökta namnservrarna använder sig av föråldrad programvara. Vi rekommenderar starkt att de verksamheter som fortfarande använder ISC BIND 8 snarast uppgraderar till senaste versionen av BIND 9, då BIND 8 är behäftad med allvarliga säkerhets- och andra brister. Leverantören Internet Systems Consortium (ISC) informerade dessutom i augusti 2007 att BIND 8 har nått "end of life" och inte längre underhålls. Det innebär att fel i programvaran, t.ex. säkerhetsbrister, inte längre kommer att åtgärdas.

BIND 9, som ersätter BIND 8, är betydligt säkrare samt har bättre funktionalitet och prestanda i jämförelse med tidigare versioner. Använder man den version av BIND som distribueras med operativsystemet så finns det med största sannolikhet en uppgradering att tillgå via den egna leverantören.

5.2.3 NAMNSERVRAR MED REKURSION PÅSLAGET

En mycket stor andel (40 %) av de undersökta namnservrarna har rekursion påslaget. Öppna rekursiva namnservrar kan komma att utnyttjas i samband med överbelastningsattacker.



Öppna rekursiva namnservrar har mycket få legitima användningsområden. En stark rekommendation är därför att eliminera möjligheten att missbruka öppna rekursiva resolvrar med hjälp av de tekniker som beskrivs i de referenser som anges i bilaga 2.

VÄRT ATT VETA

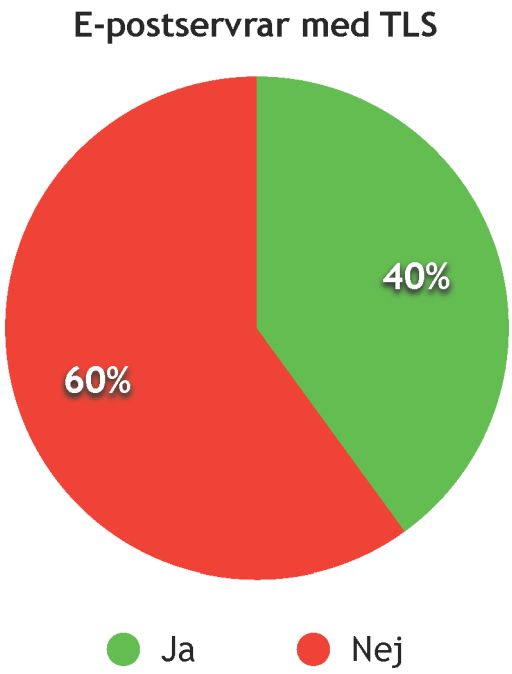
En **rekursiv namnserver** svarar inte bara på frågor om DNS-poster som den själv är ansvarig för, utan går även vidare och frågar andra namnservrar för att ta reda på svaret. Frågandet kan vara både arbetskrävande (dvs. ta datorkapacitet) och resultera i en relativt stor mängd data, vilket gör att man normalt sett vill begränsa vem som får använda funktionen rekursion.

En **öppen rekursiv namnserver** svarar på alla frågor den får där rekursion har begärts. Detta gör det möjligt för utomstående att t.ex. utföra tillgänglighetsattacker via den öppna namnservern genom att låta den ställa frågor som kommer att resultera i ovanligt stora svar. Detta i kombination med en falsk avsändaradress som leder till att svaret skickas någon annanstans kan utgöra en tillgänglighetsattack.

5.3 Viktiga parametrar för e-post

5.3.1 STÖD FÖR TRANSPORTSKYDD

Av de undersökta verksamheterna så har 40 % stöd för TLS/SSL i sina e-postservrar. Det innebär att de åtminstone teoretiskt kan skydda sin e-posttrafik mot insyn, förutsatt att de har det påslaget.



Ett testresultat som överraskade oss var när vi tittade på var verksamheterna har sina e-postservrar placerade. En avsevärd del av de undersökta verksamheterna (16 %, eller 130 av 828) har sina e-postservrar placerade utanför Sveriges gränser. Anledningen till detta är förmodligen att man anlitar någon underleverantör för filtrering av virus och SPAM.

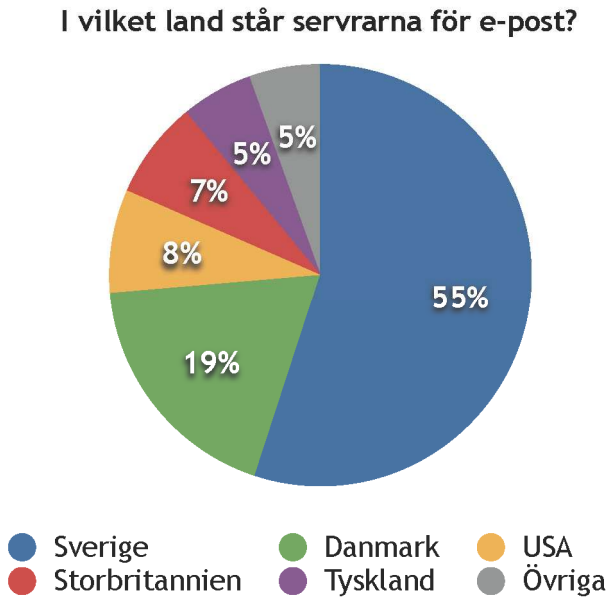
Om vi enbart tittar på kategorin svenska myndigheter så är läget vid testtillfället att 82 av dessa har sina e-postservrar i Sverige medan närmare 50 har sina e-postservrar utomlands, främst i Danmark och Tyskland men även i Storbritannien. Det innebär att en stor del av den statliga e-postkommunikationen passerar ett främmande land på sin väg till mottagaren.

Samtidigt vet vi dessutom att mycket få statliga myndigheter använder kryptering för elektronisk post. Endast 40 % av de undersökta domänerna har som tidigare nämnts utrustning som ens har möjligheten att ha kryptering aktiverad.

VÄRT ATT VETA

Överföring av elektronisk post sker vanligen i klartext och brukar därför ofta jämföras med vykort. Sedan några år tillbaka finns en standard för hur man kan överföra e-post med transportskydd, något som närmast skulle kunna jämföras med att man visserligen fortfarande skickar vykort men faktiskt låser postvagnen under själva transporten. Detta gör att någon som försöker avlyssna e-posten på vägen mellan postkontoren inte kan se vad som skickas. Transportskydd av e-post kallas ofta STARTTLS.

Om man vill skicka e-post som ingen annan skall kunna läsa, inte ens de som ansvarar för e-postsystemet (dvs. "sitter på postkontoret"), behövs ytterligare skydd. I dessa fall krypterar man hela brevet genom att man "klistrar igen kuvertet och skickar brevet rekommenderat", för att göra en analogi med traditionell postgång. De två vanligaste metoderna för denna typ av kryptering är PGP och S/MIME.



När det uppstår kommunikationsproblem mellan Sverige och omvärlden innebär det att dessa företag och myndigheter har problem att nå varandra. Placeringen av servrar i utlandet innebär också att all information passerar Sveriges gränser och att främmande stater och andra mycket enkelt kan komma åt information som kan betraktas som känslig ur olika aspekter. Det är omöjligt att säga hur medvetna verksamhetsansvariga är om att så är fallet, och om de i så fall gjort någon konsekvensanalys.

Vi kan som exempel nämna ett stort svenskt mediabolag som anlitar ett företag i Storbritannien för filtrering av sin e-post. Det innebär att all information som exempelvis lämnas till bolagets journalister passerar via det företaget i samtliga fall där journalisterna använder bolagets interna e-postsystem. Det går inte av testerna att utläsa om informationen är skyddad under transporten mellan e-postleverantören och bolaget. Vi ser dock att det finns **möjlighet** att transportskydda den information som går från bolaget till e-postleverantören. Om det omvända gäller kan vi däremot inte se.

VÄRT ATT VETA

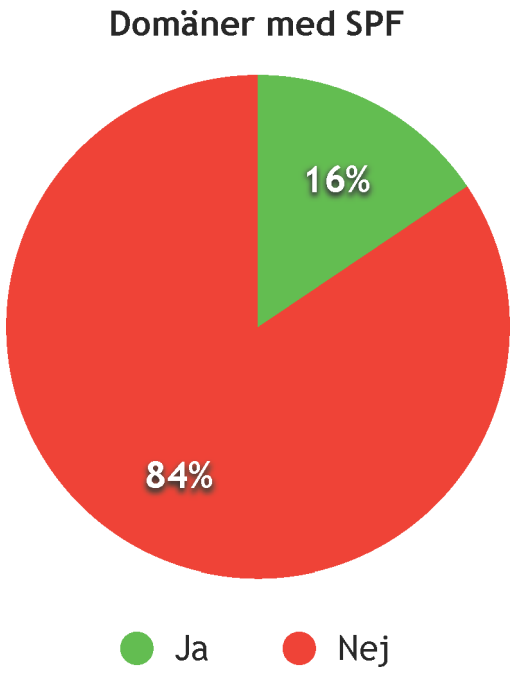
Transport Layer Security (TLS) är en öppen standard för säkert utbyte av information. TLS erbjuder konfidentialitet (kryptering) och riktighet (dataintegritet), samt beroende på användning även äkthetsskydd (källskydd). Äldre versioner av metoden benämns Secure Socket Layer (SSL).

TLS/SSL kan bl.a. användas för överföring av elektronisk post (SMTP) och vid upprättandet av en säker förbindelse mellan en webbläsare och en webbplats (HTTPS).

5.3.2 ÅTGÄRDER MOT SKRÄPPOST

Standardprotokollet för att skicka e-post, SMTP, gör det möjligt att skicka meddelanden med valfri domän som avsändaradress. SPF ger domäninnehavaren en möjlighet att i DNS publicera regler som anger från vilka datoradresser e-post från domänen ska komma. När en mottagande e-postserver får ett meddelande kontrollerar den mot SPF-informationen i

DNS hur dessa regler ser ut. Om meddelandet kommer från en sändande server som inte är publicerad i reglerna tolkas det av den mottagande servern som en indikation på att allt inte står rätt till. Den mottagande servern kan med den informationen som grund avgöra meddelandets vidare öde, till exempel vägra att ta emot meddelandet eller att sortera det som skräppost. SPF-standarden definierar inte vad som ska hända med meddelanden som **inte** klarar en SPF-validering.



Testerna visar alltså att hela 84 % av domänerna som ingått i underlaget inte använder sig av SPF, trots att detta är både förhållandevis enkelt och fullt möjligt att införa. Det innebär att det är enkelt för vem som helst att ange t.ex. en myndighets domän som avsändaradress för att lura mottagaren, utan att denne har någon möjlighet att upptäcka det. SPF tillför en sådan möjlighet till upptäckt.

VÄRT ATT VETA

Sender Policy Framework (SPF) är en metod för att motverka att meddelanden via elektronisk post skickas med falskt domännamn i avsändaradressen, dvs. att avsändaren använder någon annan adress än sin egen som avsändaradress. Läs mer om SPF på http://www.openspf.org.

En annan teknik för detta kallas Domain Keys Identified Mail (DKIM). DKIM bygger till skillnad från SPF på kryptografi, genom att avsändarens postkontor signerar (stämplar) all utgående post. Mottagarna kan i sin tur verifiera stämpeln.

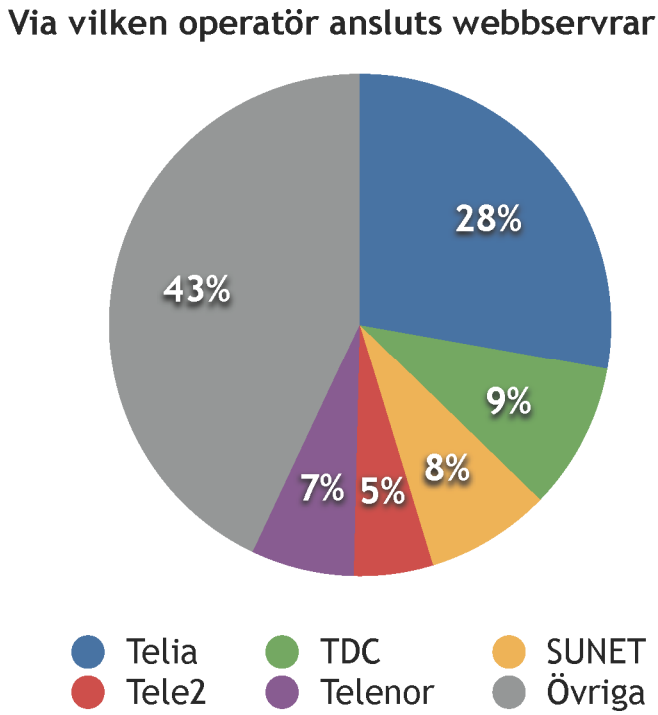
DKIM är en relativt ny standard, och används så vitt vi kan se ännu inte i någon större omfattning. Läs mer om DKIM på http://www.dkim.org.

Både SPF och DKIM syftar till att motverka nätfiske (phishing), vilket är en sorts skräppost med falsk avsändare som har som mål att lura Internetanvändare att lämna ifrån sig känslig information.

5.4 Viktiga parametrar för webb

5.4.1 ANSLUTNING AV WEBBSERVRAR

Som tidigare nämnts är det viktigt att inte placera alla ägg i samma korg. Namnservrar bör stå på olika platser, men någon av verksamhetens webbservrar bör som komplement även vara ansluten till någon annan operatör än den där verksamheten har sina namnservrar. Skälet till detta är att informationen på webbplatsen ska vara nåbar även om den egna operatören skulle få problem i sitt nät.



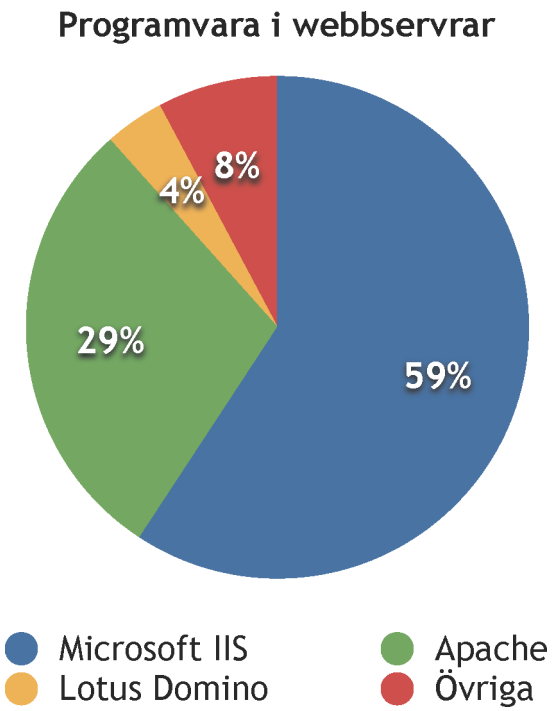
Här kan vi konstatera att testerna ger underlag för slutsatsen att det är tämligen god spridning av verksamheternas webbservrar bland operatörerna.

5.4.2 PROGRAMVAROR FÖR WEBBSERVRAR

Vi tittade på vilka programvaror för webbservrar som används i de undersökta verksamheterna. Den klart dominerande med 59 % är Microsoft Internet Information Server, Microsoft IIS. Det är en serverprogramvara från Microsoft för Internetbaserade tjänster som fungerar på nyare versioner av Windows Server.

Microsoft IIS har dragit på sig dåligt rykte som baseras på osäkerhet, då den genom åren varit en av de programvaror för webbservrar som drabbats av flest säkerhetsproblem. Det serverprogram som vunnit mest mark på senare tid är Apache.

Om vi jämför med hur det ser ut globalt så har vi i Sverige en betydligt större andel Microsoft IIS än vad som är fallet i resten av världen. Där är fördelningen den att knappt 35 % använder Microsoft IIS medan majoriteten, drygt 50 % använder Apache. (Netcraft, september 2007).



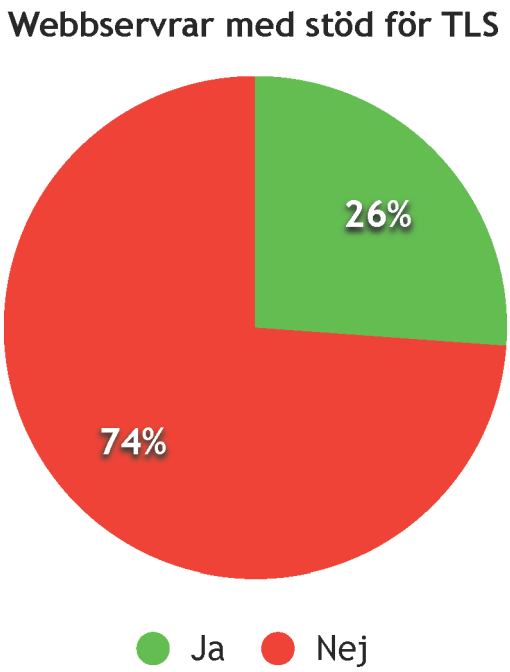
5.4.3 STÖD FÖR TRANSPORTSKYDD

För en användare som exempelvis vill komma i kontakt med en svensk myndighet eller med sin bank är det viktigt att veta att den server man har kontakt med är rätt server, att anslutningen av någon anledning inte har skett till fel tjänst eller server p.g.a. felkonfiguration eller medvetet bedrägeri.

En av de tekniker som används även för detta är Transport Layer Security (TLS) . TLS/SSL ger användarna möjlighet att kontrollera att man hamnat hos rätt server eller tjänst. (Se avsnitt 5.3.1 ovan för en beskrivning av TLS/SSL).

Webbläsaren kontrollerar adressen som uppgivits i webbläsaren med den serveradress som ingår i webbcertifikatet. Om dessa inte stämmer överens, får användaren en varning om att allt kanske inte står rätt till.

Enbart en fjärdedel av de undersökta webbservrarna har ens stöd för TLS/SSL.



Alla som via sin webbplats begär någon form av information från användare, såsom inloggning, personuppgifter, användaruppgifter, betalinformation, kreditkortsnummer, telefonnummer m.m. bör använda sig av TLS/SSL.

Med hjälp av certifikat och tillhörande krypteringsnycklar kan en webbläsare upprätta en säker, krypterad kommunikation med webbservern. Av de få verksamheter som undersökningen visar har certifikat installerade på webbservrarna använder sig en stor del av något annat än allmänt accepterade certifikatutfärdare, ofta egenutfärdade, självsignerade certifikat. Detta medför att webbplatsens besökare, dvs. användarna, inte kan verifiera om de har kommit till rätt plats. Därmed är certifikatet tämligen värdelöst.

Vi har under våra tester bl.a. sett exempel på verksamheter som har ett självsignerat certifikat utfärdat från någon okänd domän som inte förefaller ha någon anknytning till verksamheten. Vid närmare kontroll vidarebefordras man till en plats som ger ”nothing here yet” som svar – bland annat har vi stött på detta hos en svensk kommun.

En sådan användning undergräver trovärdigheten av de säkerhetslösningar som ändå finns att tillgå.

6 Råd och rekommendationer

Efter att ha genomfört dessa tester med ett tämligen dystert resultat ser vi ett starkt behov av mycket större samordning mellan olika intressenter för bättre säkerhet på den svenska delen av Internet och inte minst möjligheter till mycket stora effektivitetsvinster och kostnadsbesparingar.

I första hand verksamheterna inom den offentliga förvaltningen anser vi bör kunna enas om en tidplan för genomförandet av nedanstående aktiviteter:

- Anslut kritiska resurser i Sverige till flera operatörer samtidigt, t.ex. med användning av tekniken anycast. Det finns behov av att någon på central nivå bestämmer vad som är att betrakta som en kritisk resurs.

- Upprätta en central sekundär DNS-drift för kritiska tjänster exempelvis via de svenska Internetknutpunkterna. En sådan funktion kan regleras genom avtal.

- Upprätta en gemensam funktion för virustvätt och rensning av skräppost placerad inom landet. Det skulle bli effektivare och spara resurser. Samtidigt skulle det förhindra att myndighetsinformation lämnar landet.

- Utfärda riktlinjer om vad som är acceptabelt när det gäller skräpposthantering och virustvätt i offentlig förvaltning. Det borde inte vara accepterat att svenska myndigheter och kommuner skickar sin e-post utomlands, åtminstone inte utan att relevanta och enhetliga krav på transportskydd och kryptering ställs.

- Utfärda rekommendation om att e-postservrar för kritiska verksamheter hos svenska myndigheter och statliga verk fysiskt ska ligga inom Sverige för att skydda spårbarheten av information mellan myndigheter.

- Organisera en central nationell CA-funktion för certifikatbaserade tjänster för myndigheter. En sådan central funktion grundad på tillit kan utgöra en gemensam certifikatutfärdare för till exempel statliga myndigheter. Det är en funktion som går att upphandla hos någon etablerad och känd CA vilken kan få i uppdrag att upprätta en sub-CA för t.ex. gruppen svenska myndigheter.

- Ställ krav på offentlig förvaltning om användning av både e-post och webb med TLS för käll- och transportskydd.

Utöver ovanstående åtgärder så finns det ytterligare åtgärder som behöver vidtas bl.a. på operatörsnivå för att stärka infrastrukturen för Internet. Dessa åtgärder landar huvudsakligen på Post- och Telestyrelsen, PTS, såsom tillsynsansvarig myndighet, och handlar om att ställa krav på hos operatörerna. Vi är medvetna om att sådant arbete redan pågår, men vill ändå betona vikten av att sådana åtgärder genomförs.

Bilaga 1 - Branschstandard för DNS-tjänst med kvalitet

För den mer tekniskt bevandrade läsaren har vi redovisat mer i detalj vad vår branschstandard för DNS-tjänst med kvalitet innefattar i termer av rekommendationer.

1. Minst två namnservrar

Rekommendation: DNS-data för en zon bör ligga på minst två separata namnservrar. Dessa namnservrar bör av tillgänglighetsskäl vara logiskt och fysiskt spridda så att de är placerade på olika operatörsnät i olika autonoma system (AS).

Förklaring: För varje underliggande domän skall det finnas minst två fungerande namnservrar. De skall vara listade som NS-poster för domänen i fråga. De bör vara fysiskt separerade och placerade på olika nätsegment för att högsta funktionalitet ska erhållas. Det säkerställer att domänerna fortsätter att fungera även om någon av de aktuella namnservrarna skulle sluta fungera.

Konsekvens: När den enda servern eller den enda operatören får ett avbrott blir DNS-tjänsten onåbar för den domän som ligger på servern eller i operatörens nät. Därmed kan man inte heller nå tjänster hos domänen, även om dessa har placerats hos andra aktörer än den egna namnserveroperatören.

2. Alla namnservrar som utpekas i delegeringen skall existera i underliggande zon

Rekommendation: De NS-poster som listas i den överliggande zonen (.se eller motsvarande) för att peka ut (delegera) en viss domän skall samtliga finnas införda i den underliggande zonen.

Förklaring: I den överliggande zonen används NS-poster för att överlåta ansvaret för en viss domän till andra servrar. Denna lista av datorer skall enligt DNS-dokumentationen finnas införda även i den zonfil som "tar emot" ansvaret, och som innehåller övriga data om zonen. Listorna måste hållas synkroniserade, så att alla NS-poster som förekommer i zonfilen för toppdomänen också återfinns i den underliggande domänen. Listan i den överliggande zonfilen uppdateras inte automatiskt, utan endast efter "manuell" anmälan till ansvarig registreringsenhet. Vid förändring som leder till behov av ändring i överliggande zon skall underliggande zons administrativa kontaktperson utan dröjsmål se till att registreringsenheten meddelas om detta.

Konsekvens: Om den överliggande zonen innehåller information om den underliggande zonen som inte existerar i den underliggande zonen innebär det att den som ställer frågor om domänen inte kan få svar, med påföljd att tillgängligheten påverkas.

3. Auktoritet

Rekommendation: Samtliga namnservrar som listats med NS-poster i en delegerad zon skall svara auktoritativt för domänen.

Förklaring: Vid kontroll mot servrarna för underdomänen skall man kunna få konsistenta och repeterbara auktoritativa svar för SOA- och NS-poster för underdomänen. Detta gäller samtliga servrar som finns listade i den underliggande zonens DNS för domänen i fråga.

Konsekvens: DNS fungerar oftast även om detta fel existerar. Men att felet existerar i en zon tyder på bristande rutiner hos den som ansvarar för innehållet i DNS för den domänen.

4. SERIENUMMER FÖR ZONFIL

Rekommendation: Samtliga namnservrar som listats med NS-poster i den delegerade zonen skall svara med samma serienummer i SOA-posten för domänen.

Förklaring: Serienumret i SOA-posten är en sorts versionsnummer för zonen, och om servrarna har samma serienummer på sina zoner visar detta att de är synkroniserade. Det kontrolleras genom att fråga respektive server om SOA-posten och jämföra serienumren i svaren. SOA står för Start of Authority.

Konsekvens: Om namnservrarna inte är synkroniserade och inte har samma version av zonfilen riskerar den som ställer frågor om en domän att inte få något svar. Tillgängligheten påverkas.

5. KONTAKTADRESS

Rekommendation: Zonkontaktadressen i SOA-posten skall vara nåbar.

Förklaring: I SOA-posten för en domän ingår som andra delpost en e-postadress som ska fungera som kontaktpunkt om någon behöver nå administratören för domänen i fråga. Vid enkel kontroll skall e-postservern för e-postadressen inte ge uppenbara felmeddelanden (t.ex. ”user unknown”). Vid fördjupad kontroll ska provbrev kunna sändas till adressen och dessa ska besvaras inom tre dygn.

Konsekvens: Syftet med att ha en aktuell e-postadress för kontakter är att snabbt kunna påtala problem med nåbarheten av en domän. Om sådan inte finns kan möjligheten att lösa problem som uppstår i DNS p.g.a. någon enskild domän komma att minska.

6. NÅBARHET

Rekommendation: Alla NS-poster i den underliggande zonen ska vara nåbara för DNS-trafik från Internet.

Förklaring: NS-posterna för en domän är listan över de datorer som fungerar som namnserver för den domänen. Samtliga uppräknade servrar ska vara nåbara från Internet på alla de adresser som finns listade i motsvarande adressposter i DNS för datorerna i fråga.

Konsekvens: Om en namnserver inte är nåbar trots att den står i listan över namnservrar som svarar på frågor om en domän så innebär det att frågeställaren inte får svar. Tillgängligheten påverkas.

Bilaga 2 - Öppna rekursiva namnservrar

Grundproblemet är egentligen inte öppna rekursiva namnservrar, utan att operatörerna inte filtrerar trafik på avsändaradresser. Om de gjorde det så skulle öppna rekursiva resolvrar kanske inte betraktas som något problem. Eftersom sådan filtrering är relativt svår och kostsam att införa, så behöver vi under tiden försöka minska de skador som DDOS-attacker orsakar tills dess att operatörerna har klarat av att åtgärda grundproblemet. Att stänga en rekursiv resolver anser vi vara en enkel uppgift för många som det är värt att göra då det hjälper till att lindra de problem som uppstår vid DDOS-attacker.

Pekare till mer information

Nedan har vi samlat några länkar till bra och informativt material om DDOS och öppna rekursiva namnservrar.

Securing an Internet Name Server **http://www.cert.org/archive/pdf/dns.pdf** En bra praktisk sammanfattning för systemadministratören.

DNS Amplification attacks **http://www.isotf.org/news/DNS-Amplification-Attacks.pdf** En bra beskrivning av hur attacken går till och vad den innebär.

The Continuing Denial of Service Threat Posed by DNS Recursion **http://www.us-cert.gov/reading_room/DNS-recursion121605.pdf** Officiellt råd från USA:s CERT

ISC BIND **http://www.isc.org/sw/bind** Här finns källkod och binärer för BIND samt länkar till mycket intressant och matnyttig information.

BIND 9.3 Administrator Reference Manual **http://www.isc.org/sw/bind/arm93** Innehåller exempel på konfigurering, praktiska tips och detaljerad beskrivning av funktioner i BIND.