Robust kommunikation, har vi det?

Av Jörgen Städje

Är Internets framtid hotad? Behövs ett robustare Internet? Är inte Internet tillräckligt redundant och robust redan? Det finns de som inte bara tvivlar, utan kan bevisa att nätet har problem. Händelser i verkligheten visar om och om igen att vi har för dåligt grepp om nätets stabilitet, är dåliga på att mota angrepp utifrån och undviker att hantera kända problem.

Internet består av många aktörer som inte kan eller vill meddela sig med varandra eller med myndigheter om problem och svagheter.

Torsdagen den 4 maj var det dags att prata allvarligheter på ISOC-SEs möte hos Sunet på Tulegatan i Stockholm, när två av landets namnkunnigaste föreläsare drog till med storsläggan. Netnods säkerhetsskyddschef Patrik Fältström talade om ”Robust kommunikation på riktigt” och Internetstiftelsens säkerhetsansvariga Anne-Marie Eklund Löwinder berättade om ”DNSSEC i rotzonen”, båda lika allvarliga ämnen som man helst skulle vilja slippa höra talas om.

Varav består Internet? Är inte Internet sammansatt av alla de fina tjänsterna och användarna som använder dem, som Facebook, strömmande filmer, myndigheternas webbsidor, banktjänster och sådant? Nej, ur ett hanteringsperspektiv är Internet alla de datorhallar fyllda med servrar och routrar som ser till att koppla Internet korrekt, de databaser som talar om hur Internet ser ut och vart data ska skickas, och de hårddiskar som mellanlagrar data under tiden.

Vet man om alla dessa datorhallar är skyddade och kan motstå skarpt läge, ett angrepp från främmande makt, en större brand som ödelägger viktiga hallar, en elak grävskopa som med ett nafs tar av en stor datamotorväg? Har inte alla viktiga hallar dubbletter på andra ställen i landet? Kanske. Har inte alla hallar dubbel kraftförsörjning och reservkraft som alltid håller dem igång? Ingen vet med säkerhet. Hur länge håller reservkraften i mobilnätet när stormen Stormen kommer? Bra fråga. Har inte alla hallar dubbla fiberförbindelser som båda klarar hela trafiken om en grävskopa skulle vara framme? Vem vet? Genomför ägarna ständiga stresstester av sin strömförsörjning, intrångsskydd, åtkomlighet utifrån osv? Det kunde man ju åtminstone önska.

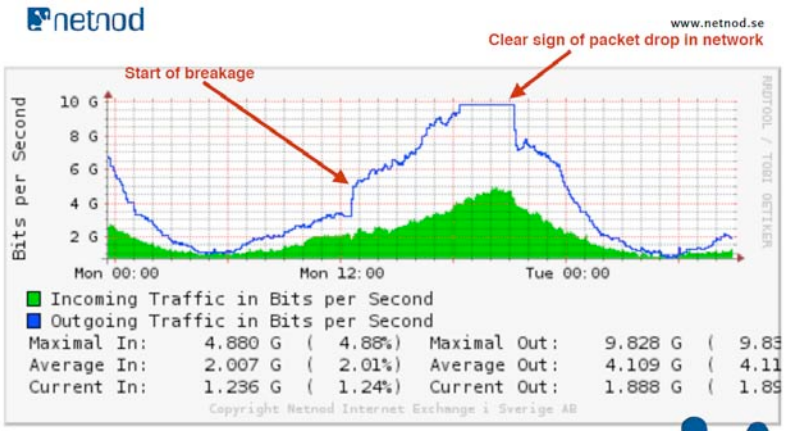
Finns det inte någon central myndighet som ska ha fullständig kontroll på detta? Nja...

Robust kommunikation på riktigt

Netnods Patrik Fältström är försiktigt diplomatisk när han beskriver statens organisation och förmåga att förebygga och avvärja ett samhällskritiskt angrepp från tredje land eller från cyberbrottslingar. De attacker vi sett mot media och myndigheter hittills har varit små, och mycket mera lurar runt hörnet.

Trafikkrisen

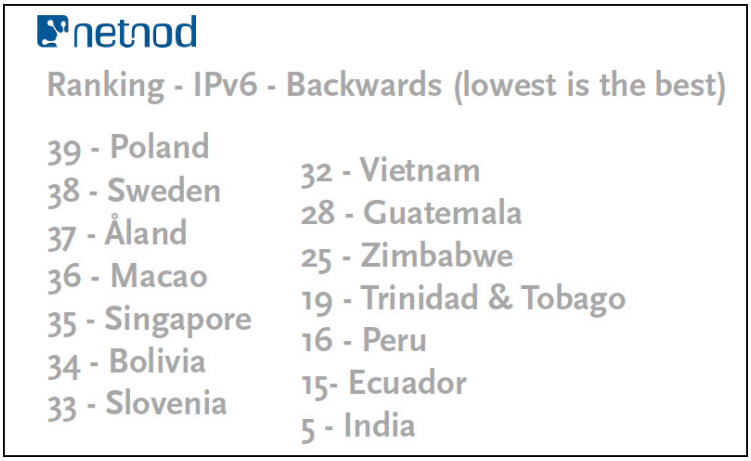
Alla vet att trafiken på Internet fördubblas var 18:e månad. ”Internet” är ett luddigt begrepp, men du kan räkna med att trafiken på dina routerportar också fördubblas var 18:e månad. Hur länge kan du hänga med i en normal situation?



Och i en katastrofsituation? En av Netnods kunder hade otur och en redundant ledning gick sönder (Start of breakage). Då växlades all trafik över på den andra ledningen just när en trafikökning var på gång. Resultatet blev att gränssnittet gick i taket och trafik fick kastas (packet drop). Plötsliga trafikökningar kan komma när som helst, till exempel i form av programuppdateringar. När man installerar Windows 10 hämtas en uppdatering på 4 GB från Microsoft. När Apple skickar ut uppdateringar till iPhone ökar nätverkstrafiken plötsligt till det dubbla. Är du förberedd?

IPv4-krisen

Att IPv4-adresserna är slut är känt sedan länge och IPv6 finns för att rädda oss. Men vi verkar inte vilja bli räddade. Det är inte längre en spekulation vad som ska hända utan krisen har övergått i kriminalitet. Organisationer stjäl andras IPv4-adresser, eller köper helt enkelt upp andra företag bara för att få deras IPv4-adressutrymme. Så här ser läget för IPv6-penetrationen i Sverige och globalt.



Man kunde tro att Sverige som är ett så tekniktungt land, skulle ligga bra till på en dylik lista men istället ligger vi på 38:e plats, efter exempelvis Grekland, Portugal och till och med Zimbabwe. Vad är det för fel på oss? Det är brist på övergripande planering och en ovilja att inse realiteter, helt enkelt.

En haverikommission behövs

Inom andra samhällssektorer, som exempelvis järnväg och flyg, har Sverige en haverikommission som undersöker haverier och levererar slutsatser om vad som måste åtgärdas för att det inte ska hända igen. Något sådant finns inte i IT-sektorn, kanske främst för att IT-leverantörerna inte vill dela med sig av information.

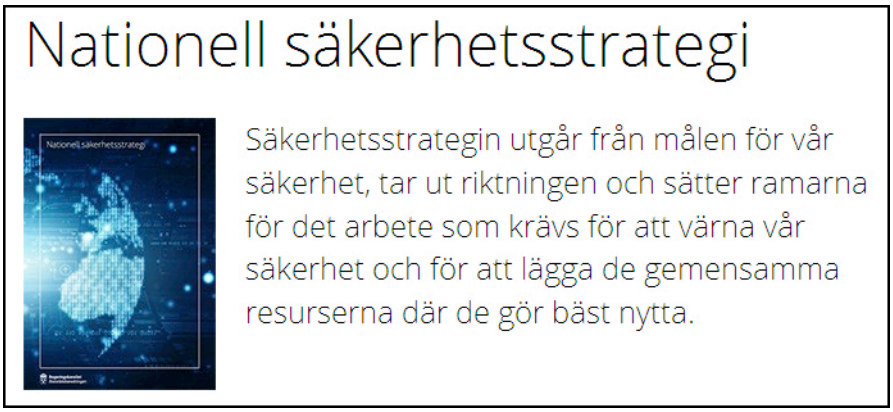
I och med molnteknikens framfart går det snart inte längre att dra gränser mellan leverantörer av data och leverantörer av den kritiska infrastruktur som transporterar data.

Tieto-kraschen år 2011 är ett exempel på en oförutsedd händelse där webbsidor och e-post slutade fungera, företag och myndigheter föll ihop och bara de som kunde och hade förberett sig kunde återgå till papper och penna. En annan följd av driftstörningen blev att många fordon fick körförbud eftersom Transportstyrelsen inte längre fick in rapporter om godkända kontrollbesiktningar, då Bilprovningen inte kunde leverera rapporter till styrelsen. Pengar kunde inte betalas ut av socialstyrelsen. Skoleleverna i Sollentuna kunde inte nå sina arbeten. Apoteket kunde inte hantera elektroniska recept och ingen vet om någon patient drabbades av detta. Däri ligger problemet: Ingen vet.

Tieto vägrade dela med sig av information till myndigheterna utan höll på sina affärshemligheter och än idag vet man inte exakt vilka som drabbades. Hur kommer det sig att

företag som har samhällsviktiga funktioner kan hemlighålla driftinformation för Myndigheten för samhällsskydd och beredskap?

Efteråt började Tieto med dubblerad lagring, katastrofövningar och riskanalysarbete. Men det var efteråt. Återgången till normal drift tog flera månader för alla inblandade.



Det är uppenbart att Sverige behöver en IT-incidentenhet (CSIRT) med makt och myndighet att kräva ut information från företag som har samhällsviktiga uppgifter, vid haverier och samhällsfarliga angrepp. Det är alldeles sant som Försvarsmakten och MSB konstaterar, att samhället måste kunna hantera destabilisering i form av antagonistiska handlingar. Det kräver att alla aktörer måste ta sitt ansvar för en god beredskap. Hur ska man få dem att göra det, frivilligt? Ladda ned skriften ovan från http://www.regeringen.se/informationsmaterial/2017/01/nationell-sakerhetsstrategi/ läs den och fundera på om den går att genomföra.

Arbetet med DNSSEC i Internets rotzon

Internetstiftelsens Anne-Marie Eklund Löwinder är en av de betrodda nyckelpigorna som har nyckeln till DNSSEC, det system som syftar till att öka säkerheten i namnöversättningen på Internet, domännamnssystemet (DNS).

DNS är en doldisfunktion som behövs för att Internet ska kunna utnyttjas av människor. En namnserver erbjuder tjänsten att tolka ett domännamn och lämna tillbaka en IP-adress som identifierar en fysisk maskin, till exempel en webbserver. En människa som vill besöka en webbplats förstår bara domännamnet ”www.sunet.se”, men det förstår inte webbläsaren som ska leta fram servern där webbplatsen ligger. Därför tar webbläsaren hjälp av den DNS-tolk (resolver) som finns närmast användaren. Med ”www.sunet.se” som indata och lämnar DNS-tolken tillbaka den verkliga, fysiska adressen 192.36.171.231.

DNS är bra – och farligt, ja, ett gift

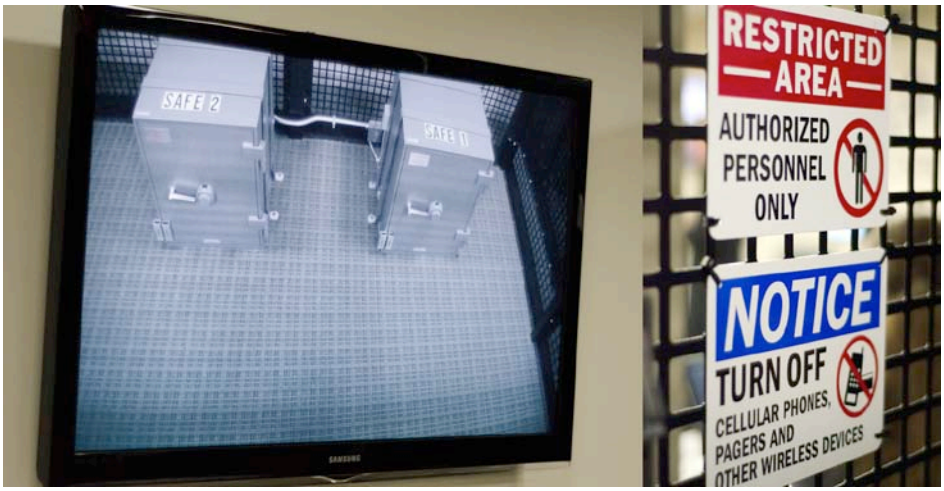
Allting på ett öppet nät kan missbrukas. Ända sedan människor i stor skala började utnyttja Internet för affärstransaktioner, bankärenden och så vidare har illasinnade krafter på olika sätt försökt exploatera det för egen vinning. Cyberkriminella kan bland annat försöka utnyttja brister i DNS för att lura intet ont anande internetanvändare.

Om man kan lura en användare genom att sabotera DNS och skicka användaren till en falsk webbplats, trots att korrekt webbadress angivits, kan man få användaren att lämna ifrån sig sekretessbelagd information, personliga data eller kreditkortsuppgifter. Att placera falska adresser i DNS-systemet kallas för att förgifta det.

DNSSEC är lösningen

DNS-servrarna ska få sitt innehåll, alltså adresser och tillhörande namn från en rotserver. Inte från en skurkserver. För att förhindra det måste DNS-servern säkras. En säkrad DNS-server tar inte bara emot adresser från rotservern utan kräver också bevis för att namnen är genuina. Beviset är en digital signatur som följer med varje adresspost. För att DNS-servern ska kunna verifiera att en riktig adress har erhållits är beviset asymmetriskt krypterat och kan packas upp med hjälp av en publikt tillgänglig kryptonyckel. Med en asymmetrisk kryptonyckel kan man bara packa upp ett bevis, inte skapa nya bevis, och därmed inte förfalska adressposter. Detta förfarande är ett tillägg till DNS som kallas DNSSEC (DNS Secure Extension).

Ett allmänt införande av DNSSEC ses av många som en nödvändighet för att Internet ska fortsätta att blomstra och utvecklas. Inte av alla tyvärr, men även om arbetet med införandet går långsamt, så går det ändå framåt.



Hög säkerhet hos IANA. Bild: Olaf Kolkman, ISOC.

Det är här nyckelpigorna kommer in. För att skapa en kedja av tillit mellan en signerad domän, via toppdomän till rotzonen behövs det ett tillitsankare. Detta ankare skapas vid en strikt ceremoni som äger rum fyra gånger per år. Ceremonierna äger rum bakom flerdubbla väggar med utrustning i kassaskåp inuti kassaskåp, under ledning av IANA (Internet Assigned Numbers Authority) i USA. Anne-Marie är den svenska betrodda representanten (Trusted Community Representative). DNS-systemet har fått vattentäta skott och i det närmaste militär säkerhet. Ceremonierna är dessutom helt transparenta och strömmas på Internet, allt för att så många som möjligt ska kunna ta del av dem och därmed känna förtroende för att allt går rätt och riktigt till.

IANA arbetar kontinuerligt med att öka trovärdigheten och acceptansen för DNSSEC. Det är också en av ISOCs såväl som ISOC-SEs främsta arbetsuppgifter.

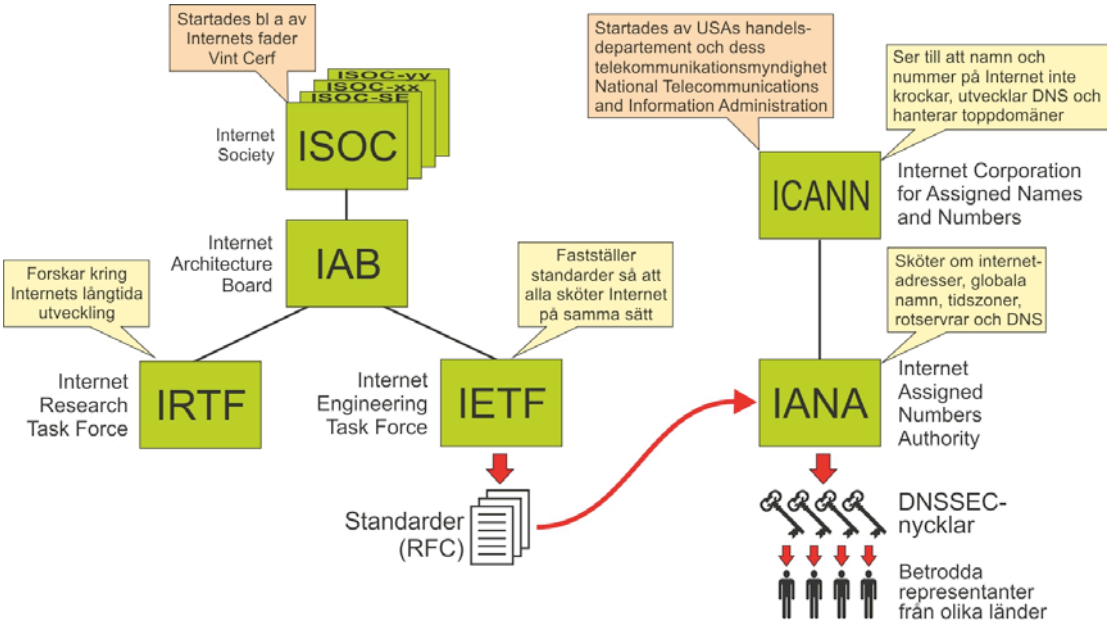
Sammanfattning

- Sverige har inte full kontroll över stabiliteten och beredskapen på Internet
- Nya cyberangrepp lurar och förvärras av vår dåliga insikt i säkerheten
- Många nätägare är dåligt förberedda på haverier och trafiktoppar
- En nationell haverikommission behövs
- DNS är osäkert och acceptansen för DNSSEC måste ökas i världen
- Införandet måste snabbas upp

Om ISOC-SE

ISOC-SE arbetar för att Internet ska fortsätta fungera som en plattform för ekonomisk och social utveckling för människor på alla håll i världen. ISOC-SE kan påverka svenska myndigheter bland annat genom remissvar och opinionsbildning och kan sprida information om viktiga internetrelaterade frågor till beslutsfattare och allmänhet samt bland egna medlemmar, till exempel på informationsmöten med anföranden av kunniga specialister inom känsliga områden. På ISOC-SEs möten får du träffa inflytelserika människor från andra organisationer och kan vara med och påverka Internets utveckling i Sverige och utomlands.

ISOC-SE är en del av internationella ISOC.



Den internationella organisationen Internet Society, med mer än 80.000 medlemmar i 110 länder, fungerar som huvudman för Internet Architecture Board (IAB) och Internet Engineering Task Force (IETF). IETF ansvarar för alla Internet-standarder och IAB tar ansvar för arkitekturen inom Internet. ISOC fyller 25 år i år och har varit drivande för öppen utveckling och för att Internet ska kunna användas av alla människor i hela världen.

För att vara vitsig kan man säga att ISOC är spindeln i nätet.

Läs mer

Om ISOC-SE: https://isoc.se/

ISOC: http://www.internetsociety.org/

Den mystiska routerkraschen: https://www.sunet.se/blogg/teknisk-djupdykning-den-mystiska-routerkraschen/

Tieto-haveriet: http://computersweden.idg.se/2.2683/1.434018/tietohaveriet---dag-for-dag

Billig Cisco-maskinvara kan vara förfalskad och stjäla ditt data: http://www.infoworld.com/article/2653167/networking/fbi-worried-as-dod-sold-counterfeit-cisco-gear.html

Läs allt om DNS och DNSSEC på svenska: https://www.iis.se/lar-dig-mer/guider/dns-internets-vagvisare/

Internetstiftelsen: https://www.iis.se/

Vill du veta mer om nyckelceremonierna kan du titta på en kort dokumentär på Youtube: https://t.co/hvbLNYmW3d