Justitiedepartementet
Enheten för lagstiftning om allmän ordning och säkerhet och samhällets krisberedskap
Stockholm den 2017-08-15

Remissvar – Informationssäkerhet för samhällsviktiga och digitala tjänster (SOU 2017:36)

Stiftelsen för Internetinfrastruktur (IIS) är en oberoende allmännyttig organisation som verkar för positiv utveckling av internet i Sverige. Vi ansvarar för internets svenska toppdomän .se, med registrering av domännamn samt administration och teknisk drift av det nationella domännamnsregistret. Sedan september 2013 sköter IIS också drift och administration för toppdomänen .nu.

IIS har fått möjlighet att lämna remissvar. IIS synpunkter begränsas till området digital infrastruktur eftersom det är inom detta område IIS verkar dels som registreringsenhet (registry) för toppdomänerna .se och .nu, dels som kunskapsnav för internetutvecklingen i Sverige. IIS står redan idag under tillsyn av Post- och Telestyrelsen (PTS) enligt lag (2006:24) om nationella toppdomäner för Sverige på Internet.

Allmänt

IIS vill i tillägg till bakgrundsbeskrivningen och den översikt som utredningen ger inledningsvis beskriva internets domännamnssystem för att tydliggöra rollfördelningen inom domännamnssystemet och därmed IIS roll.

Så fungerar internets domännamnssystem

Domännamnssystemet är den funktion på internet som ser till att det sker en uppslagning från domännamn till IP-adress och vice versa. Det är också ett exempel på att det inte existerar enskilda aktörer som ansvarar för helheten, var och en ansvarar för sin del, och genom att alla gör det fullt ut får vi en robust och stabil DNS-infrastruktur. Skälet till att det ser ut på det viset är att domännamnssystemet är uppbyggt som en hierarkisk databas vilket innebär att informationen är lagrad i en trädstruktur, som gör att det går snabbt att hitta fram till den information eller tjänst som man vill nå. Tack vare den hierarkiska uppbyggnaden behöver exempelvis de utpekade auktoritativa namnservrarna för .se (som hanteras av IIS i dess egenskap av Registry) inte ha informationen om alla .se:s underdomäner. Det ansvaret delegeras till andra auktoritativa namnservrar som hanteras av domäninnehavaren eller dennes ombud (leverantör av namnservertjänst). Varje namnserver har bara komplett information om en viss del av sin domän och denna del kallas för en zon.

Det är på detta vis man i praktiken delar upp ansvaret för internets olika delar på flera aktörer. Var och en har ansvar för DNS-informationen för sin zon. Det för med sig att domänerna längre ned i hierarkin är beroende av att de högre nivåerna fungerar, så att delegeringen verkligen sker och det går att hitta fram till den IP-adress som är knuten till ett visst domännamn. Däremot är de högre nivåerna i hierarkin inte beroende av underdomänerna. Denna ansvarsfördelning gör infrastrukturen mindre känslig. Samtidigt blir ansvaret tyngre ju närmare man kommer roten i trädstrukturen.

IIS kan till exempel bara svara för driften av innehållet i .se-zonen, men inte för driften av till exempel DNS för domännamnet regeringen.se. Det måste regeringen göra själv eller genom att anlita en tredje part som leverantör av primär namnserver.

En annan typ av namnserver är de som har till uppgift att svara på frågor om domäner i domännamnssystemet, så kallade resolvrar. Dessa innehåller inte mer information om domäner än den som tillfälligt sparas av effektivitetsskäl (cachening).

Definitioner

Utredningens förslag tar sin utgångspunkt i NIS-direktivet. Enligt NIS-direktivet är definitionen av leverantör av DNS-tjänst en enhet som tillhandahåller DNS-tjänster på internet (artikel 4.14 och 4.15).

Den definitionen är emellertid inte tillräckligt tydlig. Som framgår av beskrivningen ovan kan en DNS-leverantör vara leverantör av primär namnserver, av auktoritativ namnserver eller av resolver. Vilken eller vilka typer av namnserver som omfattas här är oklart.

Enligt utredningen omfattas NIS-direktivet också av det som benämns registreringsenhet för toppdomäner. Enligt IIS är det inte tillräckligt tydligt om det begreppet enbart omfattar det som kallas Registry (toppdomännivån) eller om det också omfattar andra leverantörer av namnservertjänster till samhällsviktiga tjänster (huvuddomännivån).

Tekniska och organisatoriska säkerhetsåtgärder

I avsnitt 7.3.1 föreslår utredningen att leverantörer av samhällsviktiga tjänster ska:

- bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete
- vidta ändamålsenliga och proportionella tekniska och organisatoriska åtgärder för att hantera risker
- vidta lämpliga åtgärder för att förebygga och minimera verkningarna av incidenter som påverkar säkerheten
- göra en riskanalys som ska ligga till grund för val av säkerhetsåtgärder.

IIS vill betona att det vilar ett tungt ansvar på ledningar och beslutsfattare, i rollerna som beställare av it-system i både privat och offentlig sektor för att göra it- och informationssäkerhet till en integrerad del av verksamheten. Att titta på hotbilden och

analysera risker är naturliga inslag. Det är dock viktigt att inse att många risker inte har sitt ursprung i antagonistiska hot, utan i det faktum att lösningar är undermåliga och ibland rentav dysfunktionella.

Enligt regeringen läggs årligen 45 miljarder kronor på it inom offentlig sektor[1] och det är enligt IIS mening nödvändigt att informationssäkerhetskraven är med från början i upphandlingsprocessen.

Det är känt sedan många år hur goda system ska vara beskaffade, hur de bör utvecklas, och hur man väljer rätt vid upphandling. Kunskaperna har många gånger bekräftats, både av forskning och i praktiken. De viktigaste lärdomarna kan sammanfattas i tre punkter:

- Utgå alltid från slutanvändarna när ett system ska byggas eller köpas in.
- Bygg it-system i små steg, sjösätt tidigt och dra lärdom av hur systemet verkligen används.
- Var beredd att ändra och göra om. Och ta med kapacitets- och säkerhetsaspekterna från början.

Ett första logiskt steg vore även att inrätta en it-haverikommission för att få bättre och faktabaserad kunskap om hur incidenter som drabbar kritiska funktioner, grupper av verksamheter eller stora delar av allmänheten ska kunna förhindras eller åtminstone lindras. En sådan kommission bör ha till uppgift att analysera händelseförloppet vid en incident med vissa specificerade egenskaper och kunna lämna konkreta förslag till åtgärder med målet att minska risken för att samma incident upprepas i framtiden.

IIS har vid flera tillfällen efterfrågat en funktion som grundligt undersöker och går till botten med vad som hänt vid en it-incident. Vi har kallat det "IT-haverikommission"[2]. En haveriutredning bör omfatta alla ingående komponenter och aktörer kring en händelse och besvara tre grundfrågor:

- Vad hände?
- Varför hände det?
- Hur undviker vi att det händer igen?

Vi pratar om en klassisk rotorsaksanalys. Kommissionen bör **inte** ha till uppgift att ta ställning i ansvars- eller skadeståndsfrågor. Arbetet ska helt enkelt gå ut på att långsiktigt förbättra säkerheten i samhällets informationssystem.

Utredningen beskriver i avsnitt 11.2.3 den föreslagna CSIRT-enhetens uppgifter och att CSIRT-enheten bland annat kan ålägga leverantörer att rapportera om incidenter. Dessutom får den behöriga myndigheten eller CSIRT-enheten - efter samråd med den rapporterande leverantören av samhällsviktiga tjänster - också informera allmänheten

---

[1] http://www.regeringen.se/regeringens-politik/digitalisering/digital-forvaltning/
[2] https://www.iis.se/docs/Remissvar-NISU-IIS-slutlig.pdf

om enskilda incidenter, om allmänheten behöver känna till dem för att det ska vara möjligt att förhindra en incident eller åtgärda en pågående incident (artikel 14.6).

Här är IIS av åsikten att CSIRT-enheten inte bara får utan faktiskt **ska** åläggas att publicera information om incidenter och tillsammans med Haverikommissionen initiera en haveriutredning som ska resultera i en rapport motsvarande den nuvarande Haverikommissionens, med beaktande av de sekretessbestämmelser som ska gälla.

Leverantör av samhällsviktiga tjänster

Inom vilka sektorer och delsektorer samhällsviktiga tjänster finns har redovisats i utredningen. MSB är förmodligen i nuläget den mest naturliga myndigheten att få ansvaret för att bedöma vilka tjänster som är viktiga för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet för var och en av de sektorer som anges i bilaga 2 till NIS-direktivet, samt att meddela generella föreskrifter och se till att dessa uppdateras minst vartannat år.

IIS instämmer i att ansvaret ska läggas på respektive verksamhet att avgöra om tillhandahållandet är beroende av nätverk eller informationssystem och om en incident skulle medföra betydande störning.

IIS instämmer även i att det ska vara tillsynsmyndigheterna som har möjlighet att utfärda de närmare föreskrifter som behövs för att fastställa om en incident medför en betydande störning eller inte.

Vilka föreskrifter som behövs måste beslutas i samråd mellan tillsynsmyndigheterna och MSB.

Säkerhetskrav och incidentrapportering – leverantörer av samhällsviktiga tjänster

Enligt utredningens förslag ska MSB vid behov få utfärda generella föreskrifter om hur ett systematiskt informationssäkerhetsarbete för samtliga sektorer kan bedrivas. Det är något som MSB har gjort sedan 1990-talet, ta som exempel FA22.[3] IIS förutsätter också att MSB själva bedriver sådant arbete för sin egen verksamhet, och därmed föregår med gott exempel. MSB har vid flera tillfällen drabbats av oväntade och onödiga avbrott i sin it-verksamhet bland annat på grund av bristande redundans i infrastrukturen.

IIS är positiv till utredningens förslag att tillsynsmyndigheten ska bemyndigas att meddela föreskrifter om utformningen av säkerhetsåtgärder. Det kan exempelvis göras genom definition av en grundskyddsnivå (baseline security) för samhällsviktiga tjänster och med säkerhetsprofiler som ska tillämpas där olika säkerhetsfunktioner ingår.

---

[3] http://users.du.se/~hjo/cs/common/doc/FA-22.pdf

När det gäller incidentrapportering är IIS av uppfattningen att det måste finnas ett klart motiv för när, till vem och hur rapporteringen ska ske. Snabb och effektiv hantering av it-incidenter har kommit att bli allt viktigare, och rapporteringen ska ses som ett medel att arbeta med förbättringar. Det får inte uppfattas som en börda för den som ska rapportera, därför bör man undvika dubbelrapportering.

IIS vill betona att gränsdragningen mellan den föreslagna lagen och redan existerande lagkrav måste bli tydligare. Om det existerar ett krav på incidentrapportering i annan lagstiftning som träffar objektet (säkerhetsskyddslagen, lagen om elektronisk kommunikation et cetera) bör enligt IIS antingen den befintliga regleringen behållas som den är, och den nya regleringen exkludera sådant som redan täcks av existerande lagar eller så måste befintliga lagar ändras så att rapporteringskravet samlas på ett ställe.

Standardisering

IIS är positiv till utredningens förslag om att leverantörer av samhällsviktiga tjänster vid utformning av säkerhetsåtgärder bör beakta europeiska eller internationellt accepterade standarder och specifikationer. IIS anser att det kravet borde vara ett skall-krav.

I andra europeiska länder, till exempel i Nederländerna[4] och i Norge har staten tagit initiativ till att rekommendera säkerhetsstandarder som behöver vara implementerade i system, framför allt för mejl och webbplatser. IIS saknar motsvarande konkreta och praktiska insatser från svenska ansvariga myndigheter. Dessutom behöver regelbundna tester göras, enkla tester kan idag genomföras med användning av öppet tillgängliga verktyg på internet.[5]

Tillsyn

IIS tillstyrker att det är mest ändamålsenligt med en tillsynsmyndighet för varje sektor.

IIS tillstyrker att PTS ska vara tillsynsmyndighet för digital infrastruktur.

IIS tillstyrker att det ska finnas ett samarbetsforum där samtliga tillsynsmyndigheter ingår samt delar samlade bedömningar av brister i informationssäkerhet i nätverk och informationssystem och andra resultat som kan vara av intresse av tillämpningen av NIS-direktivet.

Ingripanden och sanktioner

IIS tillstyrker i huvudsak de föreslagna ingripanden och sanktioner som är föreslagna. IIS saknar ett resonemang om möjligheten till reella ekonomiska incitament för genomlysning av säkerhetsbrister och till exempel offentlig redovisning av incidenter,

---

[4] https://www.ncsc.nl/binaries/content/documents/ncsc-en/current-topics/factsheets/factsheet-secure-the-connections-of-mail-servers/1/Factsheet%2BSecure%2Bthe%2Bconnections%2Bof%2Bmail%2Bservers.pdf
[5] https://zonemaster.se, https://www.hardenize.com

vilket skulle kunna skapa ett förtroendekapital hos de som ska använda tjänsterna. Sådana ekonomiska incitament kan skapas både i form av ett finansiellt stöd för leverantörer av samhällsviktiga tjänster för att nå upp till en specificerad säkerhetsnivå och som sanktion med vite för den som inte har förmågan att uppfylla de krav som ställs. Som exempel kan nämnas PTS arbete med finansiellt stöd till robusthetshöjande åtgärder i internetoperatörernas infrastruktur.

Sekretess

IIS instämmer i att sekretessfrågan kan komma att utgöra ett problem vid rapportering. Det finns en problematik särskilt för privata aktörer att känsliga uppgifter kan komma att lämnas ut och avsaknaden av en garanti att så inte kommer att ske kan innebära ett starkt hinder mot att rapportera incidenter. Det bör enligt IIS uppfattning utredas om det krävs en lagreglerad generell tystnadsplikt för privata leverantörer av samhällsviktiga tjänster. Där ställer IIS sig bakom Datainspektionens skrivelse 2017-07-07 (Dnr 1704-2017), Vissa frågor om sekretess med anledning av EU:s dataskyddsreform[6].

IIS anser att frågan om sekretess behöver hanteras samordnat med ikraftträdandet med det nya dataskyddsdirektivet i maj 2018.

Stiftelsen för Internetinfrastruktur

Dennis Aerts, vd

[6] http://www.datainspektionen.se/Documents/2017-07-13-skrivelse-sekretess.pdf