2017-08-08

Justitiedepartementet
Enheten för lagstiftning om allmän ordning och
säkerhet och samhällets krisberedskap

Netnod inkommer härmed med följande synpunkter på Remiss av betänkandet Informationssäkerhet för samhällsviktiga och digitala tjänster (SOU 2017:36)

Betänkandet föreslår hur Europaparlamentets och rådet direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen ska genomföras i svensk rätt.

Netnod har följande synpunkter:

1. Netnod anser att organisationer som redan idag täcks av adekvata krav gällande incidentrapportering och säkerhetsarbete bör exkluderas från att täckas av Lagen (2018:000) om informationssäkerhet för vissa tillhandahållare av samhällsviktiga tjänster och digitala tjänster. Vidare anser Netnod att den rapportering som krävs enligt den svenska implementationen av artiklarna 13a och 13b i direktiv 2002/21/EG (Lagen 2003:389 om elektronisk kommunikation, Förordningen 2003:396 om elektronisk kommunikation samt PTS Driftsäkerhetsarbete, inklusive, men inte begränsat till PTSFS 2012:2) är adekvata nog. Eftersom företag som tillhandahåller internetknutpunkter i Sverige täcks av Lagen om Elektronisk Kommunikation samt det nämnda driftsäkerhetsarbete bedrivet av PTS skall internetknutpunkter inte täckas av den föreslagna lagen även om direktivet är explicit på denna frågan.

   Föreslagen lag bör därför ändras (överstruken text raderas):

   > 3 § Lagen gäller inte för företag som omfattas av kraven i artiklarna 13a och 13b i Europaparlamentets och rådets direktiv 2002/21/EG av den 7 mars 2002 om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster (ramdirektiv), i lydelsen enligt Europaparlamentets och rådets direktiv 2009/140/EG~~, utom företag som tillhandahåller internetknutpunkter~~.

2. I det fall en organisation täcks av Lagen (2018:000) om informationssäkerhet för vissa tillhandahållare av samhällsviktiga tjänster och digitala tjänster och därmed blir rapporteringsskyldiga måste dessa organisationers rapporteringsskyldighet under annan tillsyn ses över så att inte dubbelrapportering krävs. Det måste även vara tydligt gällande gränsdragning i vilka fall rapportering skall ske enligt den ena eller den andra metoden. Vi anser detta speciellt skall ses över gällande företag som idag är rapporteringsskyldiga enligt PTSFS 2012:2.

3. Den föreslagna lagen (2018:000) om informationssäkerhet för vissa tillhandahållare av samhällsviktiga tjänster och digitala tjänster anger (se förslag i sektion 5.4 samt 7.3.1) att verksamhet som är av betydelse för Sveriges säkerhet skall exkluderas. Detta kan tolkas som en referens till Offentlighets- och sekretesslag (2009:400), Säkerhetsskyddslag (1996:627) och/eller Säkerhetsskyddsförordning (1996:633). Då vad som anses vara skyddsvärt är resultatet av en Säkerhetsanalys (Säkerhetsskyddsförordningen 5 §) samt att organisationer som är tillhandahållare av samhällsviktiga tjänster ofta bedriver hela eller delar av dessa med kopplingar till Säkerhetsskyddslagstiftningen måste gränsdragningen bli tydligare mellan de två regelverken, alternativt måste den föreslagna Lagen (2018:000) bli mycket tydligare hur incidentrapportering skall ske för aktiviteter som anses täckas av gällande Sekretesslagstiftning (som f.ö. håller på att ses över).

4. Då "DNS-tjänster" kan inkludera många olika saker, t.ex. de som kallas "Primär namnserver", "Auktoritativ namnserver" eller "Resolver" anser vi det är otydligt vad som avses i Förslag till lag (2018:000) om informationssäkerhet för vissa tillhandahållare av samhällsviktiga tjänster och digitala tjänster 7 § 14, och därför måste detta förtydligas.

5. Netnod anser, till skillnad från utredaren, att PTS är rätt hemvist för CSIRT då PTS enligt utredningen (avsnitt 8.5.2) skall vara tillsynsmyndighet inte bara för "Sektorn Digital Infrastruktur" utan även för "Samtliga typer av digitala tjänster". Vi anser därför CERT-SE skall i samband med ändring av uppdrag flyttas (tillbaka) till PTS.

   Netnod anser dessutom det vara mycket viktigt att den organisation som utses vara CSIRT får de resurser, den kompetens och de processer på plats som krävs för att agera på önskat sätt. Vi ser svagheter i dagens CERT-SE bl.a. i form av brist på resurser och möjlighet att själva utvärdera och dra slutsatser baserat på av andra CERT rapporterade svagheter och incidenter. Rapporter blir alltför ofta “klippa och klistra” från redan kända incidentrapporter, eller beskrivningar av att något hänt, inte tillräckligt mycket vad som hände, varför, och framför allt inte förslag på vad som ska göras för att inte samma incidenter skall hända igen. Dvs inte den summering av lärdom som Netnod anser en effektiv CERT ska göra, t.ex. ihop med Haverikommissionen (se punkt 8). Utan högkvalitativa rapporter som resultat av en CERTs arbete är incitamenten för hög kvalitet på rapporter till en CERT låg. Därför föreslår Netnod en översyn av hur CERT-SE organiseras, struktureras, bemannas samt vilka i övrigt resurser som krävs för att utföra ett fullgott arbete.

MSB ska fortfarande ha det föreslagna övergripande samordningsansvaret, men detta bör begränsas till att hantera planering och koordinering samt att vara kontaktpunkt och inte inkludera operativ verksamhet.

Förslag till förordning (2018:000) om informationssäkerhet för vissa tillhandahållare av samhällsviktiga tjänster och digitala tjänster bör därför ändras som följer:

Text som skall raderas är struken, ny text är röd:

> 8 § ~~Myndigheten för samhällsskydd och beredskap~~ Post- och Telestyrelsen är CSIRT-enhet. ~~Myndigheten för samhällsskydd och beredskap~~ Post- och Telestyrelsen ska uppfylla kraven och för Sveriges del fullgöra de uppgifter som åligger CSIRT-enheten enligt bilaga 1 till NIS-direktivet, i den ursprungliga lydelsen.
> ~~Myndigheten för samhällsskydd och beredskap~~ Post- och Telestyrelsen
> 1. ska ta emot de incidentrapporter som lämnas enligt 16 och 19 §§ lagen (2008:000) om informationssäkerhet för vissa tillhandahållare av samhällsviktiga tjänster och digitala tjänster,
> 2. ska informera andra berörda länder i Europeiska unionen om en incident som rapporterats av en leverantör av samhällsviktiga tjänster har en betydande inverkan på kontinuiteten i samhällsviktiga tjänster i det landet,
> 3. ska, om det är lämpligt, informera andra länder i Europeiska unionen som påverkats av en incident som rapporterats av en leverantör av digitala tjänster,
> 4. får informera allmänheten om enskilda incidenter efter samråd med den rapporterande leverantören,
> 5. ska när det är möjligt överlämna relevant information som kan bidra till en effektiv hantering av incidenten och det förebyggande arbetet till den rapporterande leverantören av samhällsviktiga tjänster,
> 6. ska skyndsamt uppmana leverantörer att anmäla incidenter som har sin grund i en brottslig gärning till polisen, och
> 7. ska skyndsamt överlämna de incidentrapporter som lämnats enligt 16 och 19 §§ lagen (2008:000) om informationssäkerhet för vissa tillhandahållare av samhällsviktiga och digitala tjänster till den tillsynsmyndighet som enligt 5 § denna förordning utövar tillsyn över den rapporterande leverantören~~.~~,
> 8. ska kontinuerligt överlämna rapporter och lägesbild till Myndigheten för Samhällsskydd och Beredskap.

6. Det är föreslaget i avsnitt 11.2.3 att CSIRT-enheten får informera allmänheten om enskilda incidenter. Det är vår åsikt att CSIRT-enheten ska informera allmänheten om incidenten efter samråd med inblandade parter där i detta samråd bl.a. sekretessfrågor diskuteras.

   Därför föreslås denna ändring i Förordning (2018:000) om informationssäkerhet för vissa tillhandahållare av samhällsviktiga tjänster och digitala tjänster 8 §:

   > 4. ~~får~~ ska informera allmänheten om enskilda incidenter efter samråd med den rapporterande leverantören,

7. Det är föreslaget i avsnitt 11.2.3 att CSIRT-enheten får ålägga leverantören av digitala tjänster att informera allmänheten om enskilda incidenter. Det är vår åsikt att CSIRT-enheten ska informera allmänheten om incidenten (se punkt 6 ovan) och därför sänks behovet av att leverantören skall göra det. Se även kommentar om rapporter om incidenter (punkt 8 nedan).

8. CSIRT bör kunna i samråd med Haverikommissionen göra en bedömning av säkerhetsvinsterna med en utredning. Om dessa är tillräckligt stora ska Haverikommissionen initiera en Haveriutredning som syftar till att ge svar på främst tre frågor: Vad hände? Varför hände det? Vad kan göras för att en liknande händelse inte ska inträffa i framtiden, eller för att minska konsekvenserna om den gör det? I de fall där händelsen har föranlett en insats ska utredningen också ge underlag för en bedömning av insatsen och, om det finns skäl för det, för förbättringar av dessa.

9. I definitionerna i Förslag till lag (2018:000) om informationssäkerhet för vissa tillhandahållare av samhällsviktiga tjänster och digitala tjänster 7 § 15 talas det om "registreringsenhet för toppdomäner". Som nämns på andra ställen i utredningen har vi idag redan Lagen (2006:24) om nationella toppdomäner för Sverige. Det är inte tydligt i utredningen om gränsdragning mellan dessa två undersökts eller att konsekvensanalys gjorts. Inga förslag läggs dock om förändringar av Lagen (2006:24) om nationella toppdomäner för Sverige.

   Att ha två lagstiftningar som täcker samma organisation kan fungera men är ytterligare argument för att CSIRT-funktion läggs hos PTS och inte MSB då PTS är tillsynsmyndighet för Lagen (2006:24) om nationella toppdomäner för Sverige.

10. I definitionerna i Förslag till lag (2018:000) om informationssäkerhet för vissa tillhandahållare av samhällsviktiga tjänster och digitala tjänster 7 § 15 talas om "registreringsenhet för toppdomäner". Vi vill poängtera att definitionen talar explicit om "administrerar och förvaltar registreringen" och att det därmed är den s.k. registry-funktionen för toppdomänen som beskrivs och inte den s.k. registrar-funktionen.

    Netnod anser detta är en korrekt gränsdragning och föreslår därför detta tillägg för att göra definitionen tydligare:

    > 15. registreringsenhet för toppdomäner: en enhet som administrerar och förvaltar registreringen av internetdomännamn under en specifik toppdomän, den s.k. registry-funktionen,

För Netnod

Lars Michael Jogbäck
VD