Lund, Sweden
2016-02-23
ref. 16680

Kommentarer på Statens offentliga utredningar 2015:23, Informations- och cybersäkerhet i Sverige

Bakgrund och tillvägagångssätt,

Advenica några av Advenicas samarbetspartners, har granskat SOU 2015:23 och gett kommentarer som finns sammanställda nedan. Kommentarerna syftar till att ge en så objektiv syn utifrån en svensk produktleverantörs aspekt som möjligt.

Generella kommentarer

Advenica ser positivt på utredningen som välgjord och ambitiös. På en övergripande nivå är vi eniga med ambitionsnivå, strategin och förslagen. Att inte försöka greppa över alla aspekter samtidigt är en riktig strategi. Strategin med utvalda användare och informations-säkerhetsskikt är helt riktigt för där sätts grunderna för en riktig informationshantering inom samhället i stort.

Allmänt:

1. Informationssäkerhet och cybersäkerhet
    a. Definitionen av informationssäkerhet. Sverige bör inte skilja sig från omvärlden utan vi bör presentera tillgänglighet, riktighet och konfidentialitet som de tre huvudsakliga egenskaper som informationssäkerhet avser etablera och upprätthålla. Spårbarhet (Eng. traceability) tillsammans med vissa andra, t.ex. oavvislighet (Eng. non-repudiation) nämns ibland vid sidan av eller som förslag på att de också kan ingå. Det är så ISO 27000:2014 och SIS HB 550 hanterar det. Andra standarder t.ex. NIST 800-100 tar inte upp något annat än de tre grundläggande egenskaperna. Ifall utredningen avser att etablera en svensk standard och lyfta spårbarhet till samma nivå som tillgänglighet, riktighet och konfidentialitet så bör det underbyggas, motiveras och avhandlas bättre. Det är till och med så att utredningen självt refererar till två definitioner på cybersäkerhet i kapitel 2.4.3 där samma uppdelning av ”de tre stora” görs. Inget av de inklippta citaten nämner spårbarhet. Därmed inte sagt att spårbarhet inte är viktigt, önskvärt eller värt att skydda. Det handlar enbart om att underlätta genom att följa etablerade standarder.

Konkreta kommentarer listas här nedan med referens till de sex målen.

1. Styrning och tillsyn av informationssäkerheten i staten stärks.
    a. Positivt. Förtydligande av ansvar och en koncentration och förstärkning av tillsynsansvar är ett stort steg i rätt riktning. Etablering av ett Myndighetsråd för informationssäkerhet är ett bra förslag för det skapar en defacto nivå på krav.
    b. Kommentar: Förslaget innehåller inget som klargör vilken påföljd som ska åläggas i det fall som kraven inte efterlevs.
    c. Kommentar: Som en del av uppdraget till Myndighetensrådet bör vara att ha förslag på lösningar som uppfyller kraven, (dvs kraven är obligatoriska, sedan kan myndigheter om de vill välja den föreslagna lösningen… men de kan även välja en annan väg som uppfyller kraven. Utan föreslagen lösning blir det lätt att inget blir gjort.)
    d. Kommentar. Att Myndighetsrådet ska stödja och ge råd tyder på att det kan bli ännu en mötesplats för diskussioner och kunskapsutbyte men väldigt lite konkret handling och införande.
    e. Negativt: En koncentration och nytt Myndighetsråd kan starkt bidra till mycket längre processer att besluta om åtgärder och krav. Inom detta område går utvecklingen väldigt snabbt och hotbilderna förändras nästan dagligen. Om vi som nation ska bli ledande och klara att hantera detta hot så måste besluts- och införandeprocessen blir väldigt agil. Detta är en aspekt som helt saknas i förslaget och som måste beaktas om det ska bli en förändring som inte direkt kör fast.
    f. Kommentar. En förordning för statliga myndigheter är bra. Denna förordning bör tydliggöra vilken funktion inom myndigheten som bär ansvaret för genomförande och uppföljning men bör vara noga med att inte ta helhetsansvaret från respektive myndighetschef.
    g. Kommentar. MSB har en stor roll i tillsynen. Hur denna roll kommer att ges mer tyngd är svårt att se i förslaget. MSB har haft denna roll tidigare och har kanske inte kunnat driva på förbättringar i den omfattningen som förväntas. Hur tar förslaget höjd för att förstärka denna roll rent praktiskt?
2. Staten ställer tydliga krav som upphandlare av tjänster som innehåller informationshantering eller av it-tjänster
    a. Positivt. Hänvisning av standards innebär en mer objektiv syn på kraven.
    b. Positivt. MSB framtagning av minimikrav.
    c. Positivt. Rapportering av upphandlad utrustning.

   d. Positivt. Att kunna åberopa upphandling enligt försvars- och säkerhetsområdet ger svensk industri större möjlighet att konkurrera om statliga uppdrag. För närvarande tenderar det att i praktiken endast bli pris som styr och då tillfaller en stor del av upphandlingarna bolag som är globala och har en mycket större produktportfölj. Detta ger begränsande möjligheter för små- och medelstora bolag i Sverige att konkurrera. Därmed minskar Sveriges inhemska kompetens att utveckla denna typ av lösningar vilket skapar utmaningar i de fall då säkerheten kräver lösningar framtagna inom landet.

3. Statliga myndigheter kommunicerar säkert.
   a. Kommentar. Att använda SGSI är en kortsiktig lösning där nätets svaghet ökar med antalet anslutna myndigheter. Om detta nät ska användas för all känslig information som hanteras mellan myndigheter bör det förstärkas på flera områden och en riskanalys bör göras för att optimera det för de olika tillämpningarna.
   b. Positivt: Gemensam tid är ett måste.
   c. Kommentar: Att MSB, FRA, FMV och MUST ska utveckla processer för kryptografiska funktioner är bra och görs till viss del redan. Om detta ska bli effektivt måste ledtider och tillgänglighet för leverantörer att få produkter godkända förbättras avsevärt.
4. Samtliga statliga myndigheter rapporterar it-incidenter.
   a. Positivt: IT-incident rapportering är ett måste.
   b. Kommentar: Termen IT-incidenter bör ersättas med informationssäkerhets-incidenter då detta inkluderar hanteringen av t.ex ett borttappat USB minnen som har känsliga patientjournaler eller annan känslig information.
   c. Positivt: MSB trendbevakning
5. Förebyggande och bekämpande av it-relaterad brottslighet stärks
   a. Positivt: Alla tre förslag förbättrar Sveriges möjligheter att begränsa attacker och hot.
   b. Kommentar: En insatsstyrka för informationssäkerhetsincidenter kan vara ett sätt att hantera kompetensbrist och akuta problem som riskerar kritiska samhällstjänster
   c. Kommentar: MSB bör få uppdraget att utbilda svenska folket på cybersäkerhet så att medvetenheten och kunskapen om hur man ska hantera vardagsproblematiken i sitt hem eller fritid blir bättre. I framtidens samhälle har jobb och privatliv smält ihop och ”prylar” används mellan dessa två. Generell utbildning av svenska folket skapar också en grund för opinionsbildande kring ämnet.

6. Sverige ska vara en stark internationell partner.
    a. Kommentar: För att förbättra och förstärka vår inhemska informationssäkerhetsindustri bör organisationer såsom SACS och SOFF involveras i dessa samarbeten så att det kan gagna svenska företag och deras produkt- och tjänsteutveckling.