Stockholms universitet

BESLUT
2015-09-10

Dnr SU FV-1.1.3-1689-15

Rektor

Handläggare:
Rikard Skårfors
Utbildningsledare
Planeringsavdelningen

Regeringen (Justitiedepartementet)

Yttrande över betänkandet *Informations- och cybersäkerhet i Sverige* (SOU 2015:23)

Stockholms universitet har av Regeringen (Justitiedepartementet) anmodats att inkomma med yttrande över betänkandet *Informations- och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten* (SOU 2015:23). Universitetet har följande att anföra.

Stockholms universitet tillstyrker i stort utredningens förslag. Dock menar universitetet att flera av förslagen kommer att vara starkt kostnadsdrivande för myndigheternas informationssäkerhetsarbete utan att medföra motsvarande nytta i form av minskade riskkostnader; detta då förslagen är alltför detaljerade och ställer krav på hur arbetet ska genomföras snarare än vad som ska uppnås. Universitetets invändningar rör i huvudsak den föreslagna nationella styrmodellen, detaljstyrningen kring godkända IT-produkter samt kravet på processorienterad informationsklassificering.

Sverige behöver en konkret nationell strategi inom området informations- och cybersäkerhet. Det är emellertid viktigt att strategin inte enbart pekar ut målen utan även tydliggör vad som ska skyddas, vilka aktörer som berörs, vilka roller aktörerna har, vilka åtgärder som ska vidtas, när och av vem åtgärderna ska genomföras samt hur de ska finansieras och följas upp. Beskrivningen av behovet och innehållet i den presenterade strategin är kortfattad och Stockholms universitet hade gärna sett en mer ingående redovisning av diskussioner rörande:

- hotbilder och riskanalyser som ligger bakom de prioriteringar som föreslås,
- skyddsobjekt och hur dessa uppfattas (är det huvudsakliga syftet att skydda funktioner, enskilda system, kritiska infrastrukturer eller annat?)
- de överväganden som ligger bakom utredningens fokusering på begreppet information,
- i vilken utsträckning en övergripande strategi bör inriktas på förebyggande, avhjälpande eller restaurerande insatser,
- i vilken utsträckning en övergripande strategi bör utvecklas genom tekniska, administrativa, rättsliga, polisiära eller militära medel, respektive hur dessa medel förhåller sig till varandra,

Stockholms universitet

- vilka alternativa ansvarsfördelningar och beslutsordningar som är möjliga eller av olika skäl otänkbara (inkluderande alla aktörer; jmf förslaget om inrättande av ett myndighetsråd),
- vilka argument som talar för en generell strategi och hur sådana överväganden relaterar till att säkerhetsfrågorna skiljer sig avsevärt åt inom olika sakområden.

De sex mål som preciserar betänkandets förslag till strategi är alla angelägna och Stockholms universitet har i sak ingenting att invända mot något av dem. Mot bakgrund av ovanstående punkter kan emellertid diskuteras om de angivna målen är de mest angelägna att beakta i en övergripande strategi.

Exempelvis omnämns flera gånger i betänkandet behovet av förbättrad utbildning och forskning inom informationssäkerhetsområdet. Detta utmynnar emellertid i förslag om att regeringen ska fördjupa dialogen mellan privata och offentliga aktörer samt utbildnings- och forskningsinstitutioner i fråga om utbildning och forskning inom området. Det framstår som oklart hur denna dialog ska åstadkommas, liksom hur den skulle förstärka utbildning och forskning. Från Stockholms universitets perspektiv ligger det närmare till hands att anta att forskning och utbildning stärks genom att tillföras resurser och andra former av stöd, samt av att det i den övergripande strategin finns tydligt angivna mål även för denna verksamhet.

Stockholms universitet ställer sig skeptiskt till införandet av en nationell styrmodell enligt betänkandets förslag, vilken skulle vara gemensam för samtliga statliga myndigheter. Informationssäkerhetsarbetet måste utgå från varje myndighets specifika behov och förutsättningar. Att ställa krav på gemensamma metoder för riskanalys, informationsklassificering etc. kan inte vara ekonomiskt försvarbart, och kan dessutom i sig innebära en säkerhetsrisk; förslaget om gemensamma skyddsnivåer med tillhörande skyddsåtgärder är farligt eftersom det helt ignorerar frågan om effektivitet, ändamålsenlighet, risk och andra kontextuella faktorer som bör påverka hur ett skydd ska utformas. I stället bör en nationell styrmodell vara inriktad på att tydliggöra kraven, dvs. vad som ska uppnås snarare än hur det ska uppnås. Modellen kan utformas som ett tydligare krav på efterlevnad av internationella standarder för informationssäkerhet som SS-ISO/IEC 27001.

Även om det är av stor vikt att öka kompetensen avseende kravställning vid upphandling av informationssäkerhetsprodukter inom myndigheterna är Stockholms universitet tveksamt till om den väg som föreslås i betänkandet, med införande av skyddsprofiler och hårdare styrning, är den rätta. Det bör beaktas att common criteria-certifierade produkter kan ha sämre säkerhet än motsvarande utan certifiering, samt att certifieringen i sig driver kostnader. De stora leverantörerna av IT-produkter som Microsoft, Oracle, Apple m.fl. common criteria-certifierar inte sina produkter. Flera marknadsledande IT-säkerhetsprodukter med erkänt god säkerhet är inte certifierade. Om dålig produktkvalitet vore problemet borde man rikta in sig på att köpa från leverantörer med stor kundkrets och stor säkerhetsbudget; emellertid ligger bristerna sällan i produkterna utan i avsaknad av kompetens inom installation, konfigurering, drift och förvaltning. Vad gäller kravställning vid upphandling bör man överväga att införa stöd för att

Stockholms universitet

ställa rätt säkerhetskrav snarare än att detaljstyra beställningarna på det sätt som förslaget medför.

Stockholms universitet tillstyrker förslaget att Myndigheten för samhällsskydd och beredskap (MSB) utses till tillsynsmyndighet. MSB har den kompetens och erfarenhet som krävs för att bedriva tillsyn inom området. Emellertid befarar universitetet att kostnaden för MSB:s föreslagna tillsyn är underskattad. I stället för de fem tjänster som omtalas bedömer universitetet att minst det dubbla kommer att krävas för att bedriva en tillsyn på basis av existerande och nu föreslagen författning. En modell utifrån krav på myndigheternas efterlevnad av SS-ISO/IEC 27001, där kompetens, modeller och metodik redan finns tillgängliga, skulle medföra betydligt lägre tillsynskostnader.

Det anges i betänkandet att det mesta av de föreslagna informationssäkerhetsinsatserna vid myndigheterna kan rymmas inom befintlig budget. Stockholms universitet gör emellertid den försiktiga bedömningen att myndigheternas kostnader för informationssäkerhet vid införande av modeller och processer enligt förslagen i betänkandet kommer att öka med minst 30 % på årsbasis.

Detta beslut är fattat av rektor, professor Astrid Söderbergh Widding, i närvaro av prorektor, professor Hans Adolfsson och ställföreträdande förvaltningschef, planeringschef Susanne Thedéen. Studeranderepresentanter har informerats och haft tillfälle att yttra sig. Övrig närvarande har varit Anna Riddarström, Ledningskansliet (protokollförare).

Astrid Söderbergh Widding

Rikard Skårfors