Datum
2015-09-07

Vårt diarienummer
2015-011777

Justitiedepartementet

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

Ju2015/2650/SSK

Kriminalvården har beretts möjlighet att yttra sig över betänkandet Informations- och cybersäkerhet i Sverige (SOU 2015:23) och anför följande.

1. Allmänt

Kriminalvården ställer sig i allt väsentligt positiv till förslagen som presenteras i utredningen och delar uppfattningen att informations- och cybersäkerheten i svensk statsförvaltning behöver stärkas och likriktas.

En övergripande synpunkt är att förslaget behöver samordnas bättre med förslag till ny säkerhetsskyddslag SOU 2015:25, samt Myndigheten för samhällsskydd och beredskaps föreskrift för statliga myndigheters informationssäkerhet, (MSBFS 2009:10) och dess tänkta ersättare. Kriminalvården menar att avgränsningen mellan dessa regelverk inte är helt tydlig. Kriminalvården anser bl.a. att samtliga tre förslag ska använda de definitioner och begrepp som anges i SIS TR 50-2105 för att underlätta tillämpning av och förståelse för informations- och cybersäkerhet i myndigheterna, om man inte väljer att definiera särskilda begrepp för t.ex. säkerhetsskyddslagen.

Kriminalvården är i grunden positiv till förslaget om att en nationell styrmodell förutsatt att modellen baseras på, och i linje med, svensk och internationell standard och styrmodell för informationssäkerhet (ISO 27000-serien). Kriminalvården menar att det vore olyckligt för Sveriges internationella samarbeten att inte tydligt föreskriva om tillämpning av den i Sverige och internationellt accepterade standarden för informationssäkerhet.

1.1 Informationsutbyte mellan myndigheter

Det råder idag osäkerhet gällande myndigheters möjligheter att utbyta information utifrån nuvarande bestämmelser i offentlighets- och sekretesslagen (2009:400). Utredningens förslag om en vidare utredning av huruvida en tydligare reglering kan införas i offentlighets- och sekretesslagen rörande sekretess för uppgifter som utbyts vid samverkan mellan brottsbekämpande myndigheter och andra myndigheter inom informations- och cybersäkerhetsområdet välkomnas därför. Vidare ställer Kriminalvården sig bakom utredningens bedömning att det finns flera rättsliga frågor att analysera rörande möjligheterna att samla in, lagra och utbyta information om IP-adresser inom ramen för nationella sensorsystem.

När det gäller den föreslagna strategin med tillhörande åtgärder vill Kriminalvården särskilt framhålla värdet av ett säkert kommunikationsnät för offentlig förvaltning och delar

Huvudkontoret **Säkerhetsavdelningen**

Postadress	Besöksadress	Telefon	Fax	E-post
601 80 Norrköping	Slottsgatan 78	011-496 30 00		Hk.sakerhet@kriminalvarden.se

utredningens förslag om att Swedish Goverment Secure Intranet (SGSI) kan utgöra ett sådant nät. Det som Kriminalvården saknar i detta avseende är ett förslag om att myndigheterna bör installera ett "Public Key infrastructure (PKI) så att parterna i en kommunikation kan känna tillit till att det är en behörig motpart som man kommunicerar med. Ett PKI med smarta kort och digitala signaturer minskar risken för att obehöriga bereder sig tillgång till en myndighets infrastruktur och utger sig för att vara en behörig företrädare för myndigheten både gällande intern och extern kommunikation. Sannolikt kan en sådan lösning bidra till att utveckla det elektroniska informationsutbytet mellan myndigheter med en hög grad av förtroende hos myndigheterna.

2. Specifika kommentarer till föreslagen förordning för statliga myndigheters informationssäkerhet

§ 3
Kriminalvården saknar en rimlig förklaring till att Regeringskansliet ska undantas från bestämmelserna i 11 § avseende användning av säkra kommunikationslösningar, användning av sensorsystem för IT-incidentidentifiering och kompetenskrav för informationssäkerhetschef eller motsvarande.
§ 5
Enligt förslaget krävs ett processinriktat arbetssätt, medan behovet av ledningssystem och internationella standarder endast ska beaktas. Kriminalvården anser att ett ledningssystem för informationssäkerhet enligt vedertagen standard ska föreskrivas, inte ett processinriktat arbetssätt.

§ 7
Enligt Kriminalvårdens uppfattning räcker det att föreskriva att "myndigheter ska klassificera sin information med utgångspunkt i krav på konfidentialitet, riktighet, tillgänglighet och spårbarhet". De enskilda myndigheterna kan sedan avgöra om just kartläggning av informationsprocesser är den metod som passar bäst för den egna organisationen eller om någon annan metod ska användas.

§ 8
Begreppet "säkra IT-produkter" bör definieras och utökas till att även gälla köpta tjänster. Externa tjänster nyttjas i allt större utsträckning av myndigheter som komplement till egen drift eller i stället för egen drift. Information som behandlas i myndighetsinterna system med hög säkerhet kan också helt eller delvis behandlas av externa tjänster för andra ändamål. Det är därför viktigt ur ett helhetsperspektiv att även tjänster omfattas av den förslagna definitionen.

§ 17
För att inte skapa förvirring är det av stor vikt att särskilja incidenter inom IT-området från Informationssäkerhetsområdet. I bestämmelsen avses, såvitt Kriminalvården kan förstå, det senare, d.v.s. informations- och cybersäkerhetsområdet.

I förordningen, och lämpligen i 17 §, bör också införas en övergripande bestämmelse om hur Sveriges säkerhet ska skyddas inför hotet om och effekterna av en genomförd attack mot MSB: s databas där inrapporterade incidenter lagras.

§ 18
Då Myndighetsrådet i huvudsak föreslås vara rådgivande till MSB och Regeringen har Kriminalvården svårt att bedöma hur myndighetsrådet ska kunna säkerställa verkställandet av den nationella strategin för informations- och cybersäkerhet.

Kriminalvården vill också betona det utökade behovet av praktiskt stöd från de myndigheter med särskilda uppdrag inom informationssäkerhetsområdet (FRA, FOI, Polismyndigheten och Säkerhetspolisen) som förslagen medför. Behovet av stöd från dessa myndigheter får inte underskattas och bör övervägas och lyftas fram ytterligare.

När det gäller konsekvensanalysen delar Kriminalvården uppfattningen att vissa av förslagen kan rymmas inom myndigheternas befintliga budget. Den samlade ambitionshöjningen kommer dock ofrånkomligen att medföra ett ökat resursbehov för de enskilda myndigheterna utöver de behov som redovisas för MSB. Även de förslag som presenteras avseende certifiering av säkra IT-produkter kommer sannolikt att öka kostnaderna markant för de enskilda myndigheterna.

I den slutliga handläggningen av detta ärende, som beslutats av generaldirektören Nils Öberg, har även säkerhetsdirektören Per Westberg och informationssäkerhetschefen Mats Olsson (föredragande) deltagit.

Nils Öberg

Mats Olsson

Sändlista:
Justitiedepartementet