Säkerhetspolisen

Rättsenheten

REMISSVAR

Datum
2018-04-20

Diarienummer
2018-2170-3

Mottagare
Finansdepartementet
103 33 Stockholm

Er referens
Fi2018/00106/DF

reboot - omstart för den digitala förvaltningen, SOU 2017:114

Säkerhetspolisen har följande synpunkter utifrån de intressen myndigheten har att bevaka.

Säkerhetspolisens synpunkter följer betänkandets disposition.

3 Individ och myndighet i det digitala samhället
Säkerhetspolisen instämmer i att digitaliseringen påverkar i stort sett alla delar av vårt samhälle och att det medför risker (s 65). Säkerhetspolisen tycker det är värdefullt att utredningen lyfter fram de strategiska prioriteringarna som regeringen presenterar i skrivelsen om nationell strategi för informations- och cybersäkerhet, med syfte att motverka hot i form av avsiktliga angrepp från främmande makt, terrorgrupper och kriminell verksamhet. I allt arbete som syftar till att främja digitaliseringen i samhället är det viktigt att öka kunskapen om de sårbarheter som digitalisering medför.

Utredningen nämner att offentliga myndigheter i hög grad är beroende av externa leverantörer för it-tjänster (s 66). Säkerhetspolisen har i ett flertal sammanhang påpekat att en koncentration av it-drift till ett litet antal stora leverantörer kan skapa nya sårbarheter i samhället. Den samlade informationen hos en leverantör kan bli mycket omfattande och kräver därför särskilda hänsyn från säkerhetsskyddssynpunkt. Säkerhetspolisen vill i detta sammanhang påpeka att från och med den 1 april 2018 gäller samrådsskyldighet för samtliga statliga myndigheter vid säkerhetsskyddade upphandlingar som kräver säkerhetsskyddsavtal på nivå 1. Den nya regleringen på området kan leda till att en upphandling som inte är lämplig att genomföra med hänsyn till Sveriges säkerhet stoppas. Samrådsskyldigheten kan även få konsekvenser för upphandling som avser digitalisering.

Postadress
Box 12312
102 28 Stockholm

Besöksadress
Bolstomtavägen 2
171 69 Solna

Telefon
010-568 70 00
+46-10-568 70 00

Telefax
010-568 70 10
+46-10-568 70 10

E-post/Internet
sakerhetspolisen@sakerhetspolisen.se
www.sakerhetspolisen.se

Utredningen nämner att myndigheter ska erbjuda e-tjänster när det är lämpligt (s 70). Säkerhetspolisen vill i det sammanhanget påpeka att myndighetens verksamhet är av sådan karaktär att det i vissa fall är olämpligt att använda e-tjänster och att nödvändiga möjligheter till undantag måste finnas att tillgå i lag och förordning.

9 Informationssäkerhet – en naturlig del i digitaliseringen

Säkerhetspolisen instämmer i att informationssäkerhetsarbetet inom offentliga myndigheter måste styras på ett kraftfullt sätt och genomsyra samtliga digitaliseringsprocesser (s 161-162). I detta sammanhang vill Säkerhetspolisen påpeka att det är viktigt att myndigheternas medvetenhet och kunskaper om de egna skyddsvärdena ökar.

Utredningen konstaterar att arbetet med den nationella informationssäkerheten är fragmenterat. Expert- och sektorsmyndigheter har utifrån sitt specifika ansvarsområde eller expertområde gett ut föreskrifter som i olika grad har bäring på informationssäkerhet. Säkerhetspolisen anser att arbetet med att ta fram en nationell modell för systematiskt informationssäkerhet, i enlighet med regeringens nationella strategi[1], bör prioriteras för att förbättra förutsättningarna att bedriva arbetet på ett mer samordnat sätt.

Utredningen bedömer att alla offentliga myndigheter bör omfattas av en för hela den offentliga förvaltningen gemensam reglering gällande tillsyn av informationssäkerhetsarbete med tillhörande incidentrapportering (s 167). Utredningen föreslår att Myndigheten för samhällsskydd och beredskap ska ges i uppdrag att utreda hur det kan genomföras. Det finns redan idag flera regelverk som innebär att aktörer är skyldiga att anmäla it-incidenter och att de omfattas av tillsyn (se vidare under 17.6.5). I sammanhanget vill Säkerhetspolisen därför påpeka att ytterligare krav på incidentrapportering och tillsyn kan öka den fragmentering som finns på informationssäkerhetsområdet. Det är därför viktigt att eventuell ytterligare reglering samspelar med de regler som finns idag och att den inte leder till tillämpningssvårigheter för de aktörer som omfattas.

17.6.5 Incidentrapportering

Förslaget innebär att ytterligare ett system för it-incidentrapportering åläggs aktörer som redan omfattas eller kommer omfattas av sådan skyldighet enligt andra regelverk. Det handlar till exempel om anmälan till Säkerhetspolisen eller Försvarsmakten enligt 10 a § säkerhetsskyddsförordningen (1996:633), anmälan om personuppgiftsincidenter till Datainspektionen[2], rapportering av allvarliga it-

[1] Skr. 2016/17:213

[2] Artikel 33, Dataskyddsförordningen, Europaparlamentets och rådets förordning (EU) 2016/679 samt betänkandet brottsdatalag (SOU 2017:29).

incidenter till Myndigheten för samhällsskydd och beredskap[3]. Vidare föreslås incidentrapporteringsplikt för leverantörer av samhällsviktiga tjänster i samband med införande av EU:s NIS-direktiv[4].

Systemet med parallella ordningar för incidentrapportering innebär som Säkerhetspolisen har påpekat ovan en ökad risk för fragmentering inom informationssäkerhetsområdet. Det kan även innebära att aktörer rapporterar incidenter som rör Sveriges säkerhet enligt den nu föreslagna lagen[5].

I gällande författningar, och i förslag till författningar, som avser incidentrapportering på informationssäkerhetsområdet finns undantag för incidenter som ska rapporteras enligt säkerhetsskyddslagstiftningen. Säkerhetspolisen anser att ett sådant undantag även bör gälla för rapportering av incidenter som kan påverka säkerheten i noden.

Av den föreslagna lagen bör det framgå att incidentrapportering inte tillämpas ifråga om incidenter som ska rapporteras enligt säkerhetsskyddslagen (1996:627) eller föreskrifter som har meddelats i anslutning till den lagen.

21.4 Att underlåta att skicka försändelsen digitalt via Mina meddelanden ska kräva särskilda skäl

Som Säkerhetspolisen anförde i sitt remissvar till delbetänkandet digitalförvaltning.nu (SOU 2017:23) är myndighetens verksamhet av sådan karaktär att det i vissa fall är olämpligt att skicka myndighetspost digitalt. Säkerhetspolisens verksamhet omfattas i hög grad av sekretess i t.ex. underrättelseverksamheten[6] och det kan ifrågasättas om det är lämpligt att verksamheten omfattas av en skyldighet att skicka myndighetspost digitalt. Säkerhetspolisen bör därför undantas helt från skyldigheten att skicka myndighetspost digitalt.

---

[3] 20 § förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap.

[4] Regeringens proposition 2017/18:205, Informationssäkerhet för samhällsviktiga och digitala tjänster.

[5] Lag om ändring i lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.

[6] Uppgifter i Säkerhetspolisens underrättelseverksamhet omfattas bl.a. av sekretess enligt 18 kap. 2 § offentlighets- och sekretesslagen (2009:400)(OSL). Uppgifter kan också omfattas av t.ex. försvarssekretess enligt 15 kap. 2 § OSL

Detta yttrande har beslutats av chefsjuristen Per Lagerud. Föredragande har varit verksjuristen Fredrik Sjöberg.

Per Lagerud

Fredrik Sjöberg