Datum 2015-09-15

Dnr 131 289344-15/112

Justitiedepartementet
103 33 Stockholm

Ju2015/2650/SSK

Informations- och cybersäkerhet i Sverige - Strategi och åtgärder för säker information i staten, SOU 2015:23

1 Sammanfattning

Skatteverket avstyrker utredningens förslag

- om en nationell styrmodell,
- att författningsförslaget genomförs i dess nuvarande utformning och lämnar istället ett antal förslag till förändrade bestämmelser i en sådan förordning,
- om förändring av myndigheternas internrevision enligt internrevisionsförordningen,
- om obligatorisk användning av sensorsystem för identifiering av incidenter som rör it-säkerhet (11 § andra strecksatsen) eftersom användningen av dessa sensorsystem och de rättsliga och integritetsmässiga konsekvenserna inte är närmare belysta eller analyserade,
- om en för staten speciell definition av begreppet informationssäkerhet och hävdar istället att när det gäller grundläggande begrepp som används i hela samhället är det av största vikt att statsförvaltningen beaktar nationell och internationell standard,
- om en utpekad person i myndighetens ledning med ansvar för informationssäkerhets-frågor (6 § första meningen) och lämnar istället ett alternativ,
- om bestämmelsen att kartlägga informationsprocesser (7 § första meningen),
- om att gemensamma krav- och skyddsnivåer ska användas (7 § sista meningen) och hävdar istället att den frågan inte är mogen för förordningsreglering,
- om att använda säkra it-produkter utpekade i verkställighetsföreskrifter (8 §) och hävdar istället att detta behöver beredas ytterligare då kostnadsberäkningar saknas och regeln är svår att tolka och tillämpa för myndigheterna,
- om särskilda krav på användning av säkra kommunikationsnät (11 § första strecksatsen) då kostnadsberäkningar behövs som beslutsunderlag,
- om kompetens för informationssäkerhetschef (11 § tredje strecksatsen) och menar istället att krav på informationssäkerhetskompetens hos de viktigaste myndigheterna inte ska fokuseras på en enda person eller roll,

Postadress: 171 94 Solna **Telefon**: 0771-567 567
huvudkontoret@skatteverket.se, www.skatteverket.se

- om obligatorisk incidentrapportering för vissa allvarliga incidenter och menar att vissa nödvändiga förutsättningar för ett införande fortfarande saknas, exempelvis möjligheter att med sekretess skydda tekniska uppgifter och personuppgifter,

- om upphandling och utveckling av it-system och it-produkter (15, 16 §§) och hävdar att detta behöver beredas ytterligare då kostnadsberäkningar saknas och bestämmelserna är svårtolkade,

- om att MSB utöver sina styrande och stödjande roller även ska utöva tillsyn och lämnar istället ett alternativt förslag om vidare utredning, samt

- om återrapportering i en tilläggsupplysning till årsredovisningen och menar att det är olyckligt att lyfta ut informationssäkerhet i särskilda rapporteringskrav eftersom informationssäkerhet är en av flera delar som ingår inom en myndighets ansvarsområde samtidigt som den information som myndigheter kan lämna i årsredovisningen torde vara av övergripande karaktär.

Skatteverket är angeläget om att knyta an till det som i betänkandet sägs om brottsbekämpning och då i synnerhet om tvångsmedel i den digitala miljön.

Skatteverket anser att en översyn av om en tydligare reglering kan införas i offentlighets- och sekretesslagen rörande sekretess för uppgifter som utbyts inom informations- och cybersäkerhetsområdet bör omfatta alla myndigheters uppgiftsutbyte. Tydligare sekretessreglering kan exempelvis behövas för information i incidentrapporter, respons, lägesrapporter och vid sensorsystembehandling.

Flera av förslagen riskerar att leda till mycket stora kostnadsökningar för Skatteverket och andra myndigheter. Utredningen har inte i tillräcklig grad beräknat och redovisat dessa kostnadsökningar och utgör därför inte ett adekvat beslutsunderlag. Detta är ett viktigt skäl för att Skatteverket avstyrker flera av förslagen.

2 Övergripande synpunkter

Skatteverket anser att i första hand bör regeringen använda instruktioner och regleringsbrev när det gäller att styra informationssäkerhet inom statsförvaltningen och således i största möjliga utsträckning undvika att delegera styrningen till andra myndigheter t.ex. genom bemyndiganden om att ge ut riktlinjer.

I många fall är Skatteverkets ställningstaganden beroende av hur utredningens förslag skulle kunna införas i praktiken. Skatteverket saknar erforderliga kostnadsberäkningar samt tillräcklig analys och motivering kring flera av förslagen. I de fall där en åtgärd är ytterst övergripande beskriven är det svårt att förstå åtgärdens omfattning och konsekvenser både för myndigheten och för informationssäkerheten på nationell nivå. Enligt Skatteverket behövs det tydliga förarbeten inklusive erforderliga kostnadsberäkningar till så viktiga förordningar som här föreslås.

En generell synpunkt är att förslagen både teoretiskt och praktiskt måste fungera i samspel med andra författningskrav och aktuella förslag inom angränsande områden. Detta avser inte minst SOU 2015:25 En ny säkerhetsskyddslag samt av Myndigheten för samhällsskydd och beredskap (MSB) föreslagna föreskrifter för statliga myndigheters informationssäkerhet (som ska ersätta nuvarande MSBFS 2009:10). Skatteverkets uppfattning är att utredningen har brister här alternativt att samspelet inte är tillräckligt tydligt beskrivet i betänkandet. Även i dessa avseenden utgör utredningsförslagen i fler fall ett otillräckligt beslutsunderlag.

En synpunkt som återkommer i samband med flera åtgärder gäller behovet av analys kring sekretessfrågor kopplade till åtgärden.

Skatteverket vill också betona det utökade behovet av praktiskt stöd inom området som förslagen skulle medföra om de genomförs. Detta behov får inte underskattas och verket menar att utredningen tydligare borde lyft fram frågor om hur statliga myndigheter kan få stöd inom informationssäkerhet. Exempelvis borde de stöduppdrag som MSB ska ha varit tydligare beskrivna.

3 9.1 En nationell strategi för statens informations- och cybersäkerhet, sidan 203

Skatteverket har synpunkter på flera av de förslag till åtgärder som ingår i den föreslagna strategin.

3.1 9.1.4 Strategins innehåll, sidan 208

Enligt utredningen bör en strategi för statens informations- och cybersäkerhet ha ett medellångt perspektiv som kan ligga till grund för åtgärder på två till tre års sikt. Det kan ifrågasättas om detta inte är ett väl kort perspektiv. De åtgärder som föreslås behöver i flera fall betydligt längre tid för att få effekt. Det är viktigt att arbeta långsiktigt med informationssäkerhet utan att man för den skull ger avkall på snabbt och effektivt agerande utifrån signaler ifrån verksamhet och omvärldsbevakning.

4 9.2 Ansvar, styrning, samordning och tillsyn, sidan 211

4.1 9.2.1 En nationell styrmodell, sidan 211

Skatteverket avstyrker utredningens förslag om en nationell styrmodell. Skatteverket kan med utredningens underlag inte bedöma nytta, effekt eller kostnad för Skatteverket om förslaget med en nationell styrmodell skulle genomföras. Förslaget saknar en djupare beskrivning över vad gemensamma skyddsnivåer, kravbilder och metoder betyder konkret, hur verksamhetsbehov och skillnader mellan myndigheternas verksamheter skulle kunna beaktas i tillräcklig grad samt hur förslaget skiljer sig från MSB:s nu gällande föreskrift om ledningssystem för informationssäkerhet.

Skatteverket anser även att i första hand bör regeringen använda etablerade styrformer när det gäller informationssäkerhet inom statsförvaltningen.

4.2 9.2.2 Inrättande av ett myndighetsråd, sidan 215

Myndighetsrådets uppgifter beskrivs vara mer omfattande än samverkan. Uppgiften att förebygga, följa och åtgärda brister i statens informationssäkerhet samt mandatet att förvalta och utveckla tillämpliga krav på standarder och certifiering för produkter och tjänster med bäring på informationssäkerhet i samhällsviktig verksamhet är mer långtgående än ett samverkansuppdrag.

Uppgifter som att vara remissinstans och samrådsforum för utveckling av den nationella styrmodellen, genomförare av strategi samt förvalta och utveckla krav ger myndighetsrådet en stor påverkan samtidigt som det anges att myndighetsrådet enbart ska inkludera relevanta myndigheter. Skatteverket är frågande till vilken insyn eller påverkansmöjlighet övriga myndigheter kommer att få i detta viktiga arbete.

4.3 9.2.3 En ny förordning för statliga myndigheters informationssäkerhet, sidan 220

Skatteverket avstyrker att författningsförslaget genomförs i dess nuvarande utformning. Skatteverket framför flera synpunkter som avser föreslagna bestämmelser.

4.3.1 Inledande bestämmelser (1–3 §§)

Skatteverket saknar i författningsförslaget en formulering om det ansvar för stöd till statliga myndigheter som Myndigheten för samhällsskydd och beredskap (MSB) ska ha.

4.3.2 Definitioner (4 §)

Skatteverket avstyrker författningsförslaget om en för staten speciell definition av begreppet informationssäkerhet. När det gäller grundläggande begrepp som används i hela samhället är det av största vikt att statsförvaltningen beaktar nationell och internationell standard för informationssäkerhet. Verket anser att avvikande begreppsdefinitioner försvårar förståelsen och skapar onödiga kostnader. Verket förordar att om förmåga eller spårbarhet ska betonas i samband med någon av förordningens bestämmelser bör detta i stället anges i respektive bestämmelse.

I utredningens författningsförslag förekommer flera begrepp som om dessa begrepp ska användas i en förordning behöver definieras, exempelvis god säkerhetskultur, informationsprocesser, it-incidenter, säkra kryptografiska funktioner och säkra it-produkter.

4.3.3 Regler rörande det interna säkerhetsarbetet (5–10 §§)

5 §

Skatteverket avstyrker författningsförslagets 5 § andra meningen och lämnar ett alternativ. Den andra meningen är ett allt för vagt formulerat krav angående att beakta ledningssystem jämfört med det utredningen skriver på sidan 208 om åtgärder inom strategins första mål. Även jämfört med andra motsvarande förordningskrav framstår förslaget som otydligt, jämför exempelvis 3 § förordningen (2009:907) om miljöledning i statliga myndigheter. Skatteverket föreslår därför följande alternativa formulering: *Myndigheten ska ha ett ledningssystem som omfattar informationssäkerhet och särskilt beakta etablerade standarder för informations-*

säkerhet. En sådan alternativ formulering är tydligare samtidigt som den möjliggör för en myndighet att integrera ledningssystem på ett lämpligt sätt.

6 §

Skatteverket avstyrker författningsförslagets 6 § första meningen och lämnar ett alternativ. Författningsförslagets 6 § första meningen är mer långtgående än kraven i aktuell ledningssystemstandard och förefaller oproportionerlig med hänsyn till vissa myndigheters organisation. Utredningen saknar motivering till meningens formulering. Skatteverket avstyrker därför och föreslår följande alternativa formulering: *Myndighetens ledning ska tydligt visa ledarskap och åtagande i fråga om informationssäkerhet*.

Skatteverket avstyrker författningsförslagets 6 § sista meningen och lämnar ett alternativ. I författningsförslagets 6 § sista meningen används begreppet god säkerhetskultur utan någon definition. Det begreppet är attraktivt, men det kräver mer än utbildning och övning samtidigt som det går långt utanför informationssäkerhetsområdet. Om förordningen alls ska nämna kultur i detta sammanhang föreslår Skatteverket följande alternativa formulering: *Myndigheten ska aktivt, genom utbildning och övning, verka för att en kultur etableras i organisationen där medvetenhet om informationssäkerhet ingår.*

7 §

Skatteverket avstyrker bestämmelsen i första meningen om kartläggning. Den 7 § första meningen anger att myndigheten ska kartlägga sina informationsprocesser. Skatteverket uppfattar kravet på en viss arbetsmetod som omotiverat och det odefinierade begreppet informationsprocesser som mångtydigt.

Författningsförslagets 7 § andra meningen om incidenter bör brytas ut till en egen paragraf. I meningen används det odefinierade begreppet *it-incidenter*. Begreppet it-incidenter kan misstolkas till att endast avse tillgänglighetsincidenter. Skattverket föreslår att svensk och internationell standard beaktas så att begreppet *informationssäkerhetsincidenter* används istället.

Skatteverket avstyrker författningsförslagets 7 § sista meningen om att gemensamma krav- och skyddsnivåer ska användas eftersom den frågan inte bedöms vara mogen för förordningsreglering. Verket anser att innan en för myndigheterna så ingripande reglering införs bör nivåer utarbetas och provas på frivillig väg. Se vidare synpunkter angående nationell styrmodell ovan.

8 §

Skatteverket avstyrker författningsförslagets 8 §. Texten behöver beredas ytterligare då den är svår att tolka och tillämpa för myndigheterna. Exempelvis används det odefinierade begreppet *säkra it-produkter* samtidigt som svenska myndigheter idag i allt större utsträckning anskaffar it som tjänster och inte som hårdvaruprodukter. Ett annat exempel är att formuleringen av den sista meningen inte förefaller helt förenlig med upphandlingslagstiftningen.

9 §

Författningsförslagets 9 § 1 st bör beredas ytterligare för större tydlighet. Skatteverket föreslår att orden *i en årlig plan* utgår och att stycket inleds med *Myndigheten ska årligen följa upp…*

10 §

Skatteverket avstyrker bestämmelsens föreslagna formulering. Enligt Skatteverkets uppfattning bör författningsförslagets 10 § beredas ytterligare och kraven på värdmyndigheter förtydligas.

4.3.4 Särskilda krav på informationssäkerhetsarbete (11 §)

11 §

Skatteverket avstyrker formuleringen av författningsförslagets 11 §.

Första strecksatsen kan bli kostnadsdrivande, Skatteverkets kommentarer återfinns i avsnitt Statliga nätverk nedan.

Skatteverket avstyrker den andra strecksatsen eftersom användningen av dessa sensorsystem och de rättsliga och integritetsmässiga konsekvenserna inte är tillräckligt belysta eller analyserade. Motiveringar återfinns i avsnitt angående Statliga nätverk nedan.

Skatteverket anser att den tredje strecksatsen bör beredas ytterligare. Verket menar att krav på informationssäkerhetskompetens hos de viktigaste myndigheterna inte ska fokuseras på en enda person eller roll.

4.3.5 Säkra kryptografiska funktioner (12–14 §§)

Skatteverket anser att definitionen av säkra kryptografiska funktioner i krisberedskapsförordningen (2006:942) ska flyttas med om dessa regler flyttas till en ny förordning.

4.3.6 Upphandling av it-system och it-produkter (15–16 §§)

15 §

Skatteverket avstyrker författningsförslagets 15 §. Författningsförslagets 15 § 4 st behöver beredas ytterligare. Stycket överensstämmer inte med 10 kap. 2 § offentlighets- och sekretesslagen (2009:400). Författningsförslagets ordval *ska endast* bör ersättas med *får endast*. Här som i förordningen i sin helhet bör begreppet *it-incidenter* bytas ut.

16 §

Skatteverket avstyrker författningsförslagets 16 §. Skatteverket är positivt till standardisering. Den här bestämmelsen är dock både svårtolkad och oproportionerligt kostnadsdrivande då samhällsviktig verksamhet utgör en omfattande del av de statliga myndigheternas verksamhet. Texten behöver beredas ytterligare då den är svår att tillämpa för myndigheterna. Exempelvis används det odefinierade begreppet *säkra och certifierade it-produkter* samtidigt som

svenska myndigheter idag i allt större utsträckning anskaffar it som tjänster istället för som hårdvaruprodukter. Ett annat exempel är att formuleringen av den sista meningen inte förefaller helt förenlig med upphandlingslagstiftningen.

4.3.7 It-incidentrapportering (17 §)

17 §

Trots att frågan om obligatorisk incidentrapportering utretts tidigare är det Skatteverkets bedömning att det fortfarande saknas vissa nödvändiga förutsättningar för ett införande via förordning. Viktiga förutsättningar är förutom tekniska stödsystem och tillräckliga resurser även möjligheter att med sekretess skydda vissa tekniska uppgifter och personuppgifter som kan förekomma både i incidentrapporterna och i den returinformation som den rapporterande myndigheten behöver få tillgång till. Motiveringar återfinns i avsnittet Incidentrapportering nedan.

4.3.8 Tillsyn, föreskrifter, Myndighetsrådets uppgifter (18–20 §§)

18 §

Skatteverkets synpunkter framgår av avsnitt om Inrättande av ett myndighetsråd ovan.

19 §

Skatteverket avstyrker författningsförslaget i denna del. Se avsnitt om Tillsyn nedan för motivering och förslag till vidare utredning.

20 §

Skatteverket avstyrker författningsförslagets första och fjärde bemyndiganden. Mot bakgrund av vad Skatteverket anfört angående de bestämmelser som bemyndigandena avser är dessa bemyndiganden allt för långtgående.

Författningsförslagets tredje bemyndigande är svårtolkat vilket Skatteverket även påpekat angående 16 § ovan.

4.4 9.2.4 Tillsyn, sidan 227

Skatteverket avstyrker utredarens förslag om att MSB ska utöva tillsyn och lämnar ett alternativt förslag om vidare utredning. Skatteverket delar inte utredarens syn att den bästa lösningen är att MSB utöver sina styrande och stödjande roller även bör ges rollen att utöva tillsyn inom området.

Skatteverket vill påpeka följande svagheter i utredarens lösning. Det förslag till ny säkerhetsskyddslag som nu remissbehandlas föreslår att säkerhetsskyddslagen ges en bredare tillämpning. Därmed skulle en förstärkt tillsyn innebära en ökad belastning och risk för dubbelarbete för många myndigheter som blir föremål för överlappande tillsyn från både Säkerhetspolisen och MSB inom informationssäkerhet. Det kan även tänkas att tillsyn från

MSB i vissa fall kan hindras av sekretess med hänsyn till säkerhetsskydd och Sveriges säkerhet. En svaghet med förslaget är att den stödjande roll som MSB har kan försvagas om både den styrande rollen förstärks och en ny tillsynsroll tillkommer. Detta kan ske om MSB stegvis skulle anpassa sitt stöd utefter de nya uppdragen med utökad styrning och tillsyn. Detta skulle sannolikt orsaka en negativ effekt på informationssäkerhetsarbetet inom statsförvaltningen då det inte finns någon annan myndighet som stödjer myndigheterna i samma omfattning. Betänkandet ger inte heller stöd för att övriga förslag skulle kompensera för effekten av uppdraget med tillsyn.

Skatteverkets alternativa förslag om tillsynssamverkan

Skatteverket bedömer att det krävs samverkan mellan tillsyn av statliga myndigheters informationssäkerhet och tillsyn av myndigheternas säkerhetsskydd. Även utredaren pekar på behovet av viss översyn i samband med behovet av samordning med sektorsvis tillsyn.

Skatteverket föreslår därför att regeringen låter utreda lämpliga former för samverkan när det gäller all tillsyn över statliga myndigheters informationssäkerhet inklusive säkerhetsskydd och avstyrker utredningens förslag om att MSB ska utöva tillsyn.

4.5 9.2.5 Informationssäkerhet som en del av myndighetens revision, sidan 230

Skatteverket avstyrker utredningens förslag i dessa delar.

Förslag om myndigheternas internrevision enligt internrevisionsförordningen

Skatteverket är en av de 66 förvaltningsmyndigheter som ska ha en internrevision inrättad i enlighet med bestämmelserna i internrevisionsförordningen. För övriga myndigheter finns inget krav på internrevision.

Bestämmelserna i internrevisionsförordningen är kopplade till internationella standarder för internrevision som ges ut av The Institute of Internal Auditing (IIA). Utgångspunkten för om en revision ska ske är en bedömning av verksamhetens risker. Riskanalysen ska omfatta all verksamhet som myndigheten bedriver och ansvarar för och ska utmynna i en prioritering av granskningsområden utifrån risk och väsentlighet. Eftersom informationssäkerhet är ett bland många andra områden som ingår i myndighetens ansvarsområde kommer internrevisionens riskvärdering för detta specifika område att ställas i relation till alla de övriga. Beslut om revisionsplan fattas av uppdragsgivaren som för Skatteverkets del är generaldirektören.

Utredningens bedömning om att revisionen av informationssäkerhet bör utvecklas saknar underlag som beskriver vilka brister som finns och det finns i utredningen oklarheter kring vad som avses med internrevision.

Internrevisionsförordningen ger inte utrymme för den typ av granskning som utredaren föreslår. Skatteverket avstyrker därför utredningens förslag.

Förslag om ledningens roll och brister i uppföljning

Utredningen och tidigare rapporter påvisar att det kan finnas brister när det gäller statliga myndigheters uppföljning av sitt ledningssystem för informationssäkerhet.

Interna ledningssystemrevisioner ska enligt aktuell standard ske med planerade intervall för att myndighetsledningen ska få information om huruvida ledningssystemet för informationssäkerhet

a) överensstämmer med organisationens egna krav på sitt ledningssystem för informationssäkerhet; och kraven i svensk och internationell standard samt
b) har införts och underhållits på ett ändamålsenligt sätt.

Om denna del av standarden inte följs i tillräcklig omfattning är det enligt Skatteverkets mening i första hand föreskrifterna från MSB som skulle kunna förtydligas. Utredningen lägger dock inget tydligt förslag om detta.

Det som finns är författningsförslagets 6 § första meningen som är mer långtgående än kraven i aktuell ledningssystemstandard och förefaller oproportionerlig med hänsyn till vissa myndigheters organisation. Utredningen saknar motivering till meningens formulering. Skatteverket avstyrker därför och föreslår istället följande alternativa formulering: *Myndighetens ledning ska tydligt visa ledarskap och åtagande i fråga om informationssäkerhet.*

Slutligen lägger utredningen ett alternativt förslag om att i myndighetsförordningen (2007:515) införa en bestämmelse om att myndighetens ledning ansvarar för att upprätthålla säkerhet i sin informationshantering. Med hänsyn till skrivningen i § 3 i myndighetsförordningen finns redan reglerat att myndighetens ledning ansvarar för verksamheten och att den ska se till att verksamheten bedrivs effektivt och enligt gällande rätt. Nyttan med åtgärden för att nå eftersträvade effekter bedömas som ringa.

Förslaget om återrapportering

Utredningen föreslår att det i förordningen (2000:605) om årsredovisning och budgetunderlag införs en bestämmelse om att till årsredovisningen en tilläggsupplysning ska lämnas om genomförd internrevision och status för informationssäkerhetsarbete på myndigheten. Förslaget till åtgärd torde medföra en något utvidgad löpande uppföljning samt att ett nytt område får läggas till och redovisas som ett övrigt återrapporteringskrav i årsredovisningen.

Skatteverket menar dock att det är olyckligt att lyfta ut informationssäkerhet i särskilda rapporteringskrav eftersom informationssäkerhet är en av flera delar som ingår inom en myndighets ansvarsområde. Den information som alla myndigheter kan lämna i årsredovisningen torde vara av övergripande karaktär. Om regeringen önskar mer ingående information om risker och sårbarheter som rör informationssäkerhet, från vissa myndigheter som hanterar känslig information och där det bedöms föreligga ett behov av ökat engagemang, kan ett uppdrag i regleringsbrev alternativt infört i myndighetens instruktion användas. Rapporteringen görs lämpligare i ett sammanhang då sekretessreglering finns exempelvis i samband med risk och sårbarhetsanalys enligt krisberedskapsförordningen.

5 9.3 Staten som tydlig kravställare, sidan 235

5.1 9.3.1 Kravställning vid upphandling, sidan 236

Skatteverket avstyrker författningsförslagets 15 - 16 §§. Skatteverket är positivt till standardisering, men avstyrker utredarens förslag då underlaget är alltför bristfälligt bland annat avseende kostnadsberäkningar. Förslaget är också allt för svepande och svårtolkat för reglering i förordning och verkställighetsföreskrifter. Skatteverket har därför ej kunnat bedöma eventuella konsekvenser i form av nytta och kostnader av förslaget även om det står klart att förslaget på kort sikt medför ökade kostnader.

Betänkandet anger att vanligt förekommande it-produkter ska inkluderas. Statliga myndigheter ser en utveckling där en större andel tjänsteupphandlingar är påtaglig. Det finns utmaningar i att utforma regler och säkerhetskrav vid upphandling som står i samklang med upphandlingslagstiftningen.

Utredningen har inte konkretiserat vad av detta stora produkt- och tjänsteområde som ska regleras. Allvarliga konsekvenser kan uppstå om styrande regler tvingar vissa myndigheter att avropa så kallade certifierade säkra produkter. Skulle detta innebära att Skatteverket inte längre kan nyttja på marknaden etablerade it-produkter kan det få allvarliga konsekvenser för verksamheten. Den certifierade produktfloran är idag klart begränsad och myndigheterna kan få utmaningar med kompetensförsörjning kring sådana produkter då dessa idag i första hand används inom försvaret.

Förslaget om att införa krav om att rapportera vilken leverantör som valts då avrop sker från ramavtal innebär inga större konsekvenser för Skatteverket. Skatteverket vill dock framhålla att ett sådant förslag endast ger en förbättrad lägesbild över eventuella sårbarheter. Hur sårbarheten eller risken ska minskas berörs inte i betänkandet. Om en sådan rapport-bestämmelse ska införas bör dess syfte och mål vara tydligt beskrivna i förarbetet så att också den tänkta effekten av förslaget kan bedömas.

6 9.4 Säkrare kommunikation i staten, sidan 246

6.1 9.4.1 Statliga nätverk, sidan 246

6.1.1 Utvecklade kommunikationssystem för säkrare kommunikation i staten, sidan 248

Skatteverket är anslutet till SGSI. Verket anser dock inte att det är effektivt eller lämpligt att styra användningen av SGSI genom förordning och föreskrifter från MSB och avstyrker därför förslaget.

Som nämnts tidigare kan författningsförslagets 11 § första strecksatsen om obligatoriskt användande av SGSI bli kostnadsdrivande beroende på hur den regeln tillämpas. Att SGSI idag används i så liten utsträckning av anslutna myndigheter beror troligen på att myndigheter sett liten nytta i att för varje it-system utveckla och förvalta stöd för en alternativ kommunikationsväg via SGSI till ett fåtal myndigheter när andra befintliga lösningar finns för kommunikationen med allmänhet, företag och myndigheter. Kostnaden för

användningen av SGSI är hög jämförd med motsvarande kommersiella lösningar. Myndigheter som erbjuder samhället e-tjänster såsom Skatteverket måste ha stabil publikt åtkomlig infrastruktur för att hantera den stora kapacitet som behövs vid de tillfällen under månaden och året då information enligt lag ska tas emot och eller hanteras.

Utredningen resonerar om behovet av utveckling av SGSI på olika sätt. Skatteverket vill dock i detta sammanhang påpeka att hittills har stora delar av den offentliga sektorns datakommunikation inte alls haft möjlighet att använda SGSI eftersom privata företag inte kunnat anslutas även om dessa utför omfattande informationsbehandling som personuppgiftsbiträden åt statliga myndigheter, landsting och kommuner.

6.1.2 Sensorsystem, sidan 250

Skatteverket avstyrker förslaget om obligatorisk användning av sensorsystem för identifiering av incidenter som rör it-säkerhet. Detta görs eftersom användningen av dessa sensorsystem och de rättsliga och integritetsmässiga konsekvenserna inte är närmare belysta eller analyserade.

Av betänkandet framgår att man med sensorsystem avser en kommunikationslösning med tekniska sensorer och en central funktion för analys av de avvikelser som uppmärksammas av sensorerna. Sensorerna skannar den trafik som går till och från t.ex. Skatteverket och om någon information aktiverar sensorerna går ett larm till en central analysfunktion och eventuellt även vidare till den verksamhet som blivit utsatt för ett it-angrepp.

Vilka särskilda krav på sensorsystem som ska ställas på myndigheterna anges inte. Av 20 § i författningsförslaget framgår dock att MSB får meddela de föreskrifter som behövs för verkställigheten av de allmänna och särskilda krav på statliga myndigheters informationssäkerhetsarbete som bl.a. avses i 11 §.

Användning av sensorssystem innebär, om de ska användas på kommunikation till och från Skatteverket, behandling av personuppgifter. Användningen innebär också att, för det fall någon central funktion för analys utnyttjas, t.ex. FRA, att sekretessreglerad information kommer att hanteras utanför den verksamhet där informationen är skyddad av sekretess. I utredningens övervägande påtalas att vissa rättsfrågor inom områdena sekretess och personuppgiftsbehandling måste analyseras ytterligare. Någon egen analys har utredningen inte redovisat.

Enligt Skatteverkets uppfattning måste man ifrågasätta det lämpliga i att utredningen inte gjort någon egen analys av viktiga integritets- och sekretessfrågor som aktualiseras i det författningsförslag som man lägger fram. Vem förväntar sig utredningen ska göra dessa analyser när författningsförslaget öppnat för detaljreglering genom myndighetsföreskrift?

Skatteverket ser det som rimligt att anta att en bred övervakning genom sensorsystem av den elektroniska trafiken till och från myndigheter kan skapa förtroendeskadliga situationer för både enskilda myndigheter och för e-förvaltningen. Särskilt som användningen av dessa sensorsystem och de rättsliga konsekvenserna inte är närmare belysta eller analyserade. Någon allmän diskussion kring övervakningen av elektronisk trafik mellan myndigheter och

mellan myndigheter och enskilda har inte heller förts vilket i sig kan skapa frågor kring enskildas förtroende för myndigheternas hantering av information.

6.2 9.4.2 Säkra kryptografiska funktioner, sidan 254

Utredningen föreslår att utveckla processen för säkra kryptografiska funktioner för användning vid kommunikation internt inom statsförvaltningen. Skatteverket vill dock understryka att de statliga myndigheterna även har ett växande behov av att skydda kommunikation med utländska myndigheter samt med enskilda såväl i Sverige som i utlandet. Utredningen ger inget stöd när det gäller kompetens och samverkan vid val av produkter och lösningar i dessa sammanhang.

7 9.5 Incidentrapportering, sidan 257

Skatteverket avstyrker förslaget eftersom vissa nödvändiga förutsättningar för ett införande fortfarande saknas. Trots att frågan om en obligatorisk incidentrapportering utretts tidigare är det Skatteverkets bedömning att det fortfarande saknas vissa nödvändiga förutsättningar för ett införande via förordning.

Viktiga förutsättningar är förutom tekniska stödsystem och tillräckliga resurser även möjligheter att med sekretess skydda vissa tekniska uppgifter och personuppgifter som kan förekomma både i incidentrapporterna och i den respons som den rapporterande myndigheten behöver få tillgång till. Betänkandet innehåller inte tillräcklig information om vad som ska rapporteras utan anger allmänt att det avser *it-incidenter som allvarligt kan påverka säkerheten i den informationshantering som myndigheten ansvarar för.* Då betänkandet därutöver föreslår att MSB ska få ett öppet bemyndigande att föreskriva hur ett genomförande bör ske kan Skatteverket inte bedöma konsekvenser av förslaget i dess nuvarande form.

Skatteverket ser en utmaning då incidenter inträffar som berör informationssystem som omfattas av säkerhetsskydd och då särskilt när it-infrastruktur omfattas. Det är inte ovanligt att händelseförloppet för en incident är utsträckt och det är inte alltid känt initialt vilka tillgångar och system som är berörda. Av detta skäl riskerar osäkerhet eller felaktigheter uppstå då det ska beslutas till vilken myndighet incidenten ska rapporteras. Skatteverket föreslår att särskild hänsyn tas till detta om förslaget bereds vidare.

Skatteverket ser även för förslaget om informationssäkerhetsrelaterade lägesbeskrivningar, ett möjligt behov av sekretessreglering för vissa uppgifter.

8 9.6 Brottsbekämpning, sidan 262

Skatteverket är angeläget om att knyta an till det som i betänkandet sägs om brottsbekämpning och då i synnerhet om tvångsmedel i den digitala miljön.

8.1 9.6.1 It-brottskonventionen, sidan 262

Verket instämmer i att Europarådets konvention om it-relaterad brottslighet bör ratificeras. På sikt bör fler myndighetsområden komma i fråga för sådant reglerat samarbete som krävs med den så snabbt ökande internationella digitaliseringen.

8.2 9.6.2 Informationsutbyte, sidan 263

Skatteverket anser att alla myndigheters uppgiftsutbyte bör omfattas av den översyn som föreslås om en tydligare reglering i offentlighets- och sekretesslagen rörande sekretess för uppgifter som utbyts inom informations- och cyber-säkerhetsområdet. Tydligare sekretessreglering kan exempelvis behövas för information i incidentrapporter, respons, lägesrapporter och vid sensorsystembehandling.

8.3 9.6.3 Översyn av bestämmelser om tvångsmedel i den digitala miljön, sidan 264

Skatteverket är angeläget om att knyta an till det som i betänkandet sägs om brottsbekämpning och då i synnerhet om tvångsmedel i den digitala miljön.

Som konstateras i betänkandet sker elektronisk lagring av uppgifter i allt större utsträckning på annan plats än där personer eller verksamheter finns och det sker allt oftare på en server som finns i utlandet. Härtill kommer att bilden kompliceras ytterligare genom de snabbt ökande s.k. molntjänsterna, där uppgifterna kan vara lagrade var som helst i världen - på en eller flera platser. Många gånger är dessa uppgifter digitalt låsta, i den meningen att de inte är öppet tillgängliga för envar på internet.

Som också är vanligt i andra sammanhang omnämns i betänkandet främst de straffprocessuella tvångsmedlen, reglerade i rättegångsbalken. Genom skatteförfarandelagen – och tidigare författningar – har också Skatteverket befogenhet att eftersöka och omhänderta handlingar. Sådan bevissäkring får ske efter medgivande av domstol. Vid en tidig prövning har Högsta förvaltningsdomstolen funnit att ett sådant medgivande till sin karaktär kan jämföras med ett beslut om husrannsakan under en förundersökning. Både inom och utom Skatteverket har i dessa sammanhang väckts viktiga frågor om myndigheters befogenheter.

Bland ytterligare, besläktade befogenheter kan nämnas Konkurrensverkets undersökningar och de allmänna domstolarnas prövning av begäran om upphovsrättsliga intrångsundersökningar.

Särskilt på områden utanför det straffprocessuella råder brist på rättsregleringar och rättspraxis och det finns bland olika myndigheter inget självklart gemensamt synsätt. Uppfattningar om nödvändig rätt till en direkt, gränsöverskridande åtkomst förs fram.

I ärenden om sådan övrig tvångslagstiftning som berör myndigheters tillgång till handlingar och uppgifter har det mycket sällan gjorts uttalanden om digital lagring och om att denna inte längre sker på den fysiska platsen för undersökningen.

Skatteverket instämmer i att det behövs en genomgripande och detaljerad genomgång och analys och vill framhålla att det är viktigt att även andra tvångsmedel än de straffprocessuella inbegrips. En förnyad utredning om tillämpning av tvångsmedel i den digitala miljön skulle vara värdefull.

9 Konsekvenser av förslagen, sidan 277

Som anges på sid 277 innebär utredningens förslag ökade krav på och en höjd ambitionsnivå för statens informationssäkerhet. Skatteverket anser att det saknas adekvata kostnadsberäkningar. Skatteverket anser det inte vara relevant eller korrekt att (sid 282) framhålla att kostnaderna kan antas vara marginella jämfört med de totala verksamhetskostnaderna.

Flera av förslagen riskerar att leda till mycket stora kostnadsökningar för Skatteverket och andra myndigheter. Utredningen har inte i tillräcklig grad beräknat och redovisat dessa kostnadsökningar och utgör därför inte ett adekvat beslutsunderlag. Detta är ett viktigt skäl för att Skatteverket avstyrker flera av förslagen.

Exempel på förslag som skulle medföra ökade kostnader är följande:

- Kravet i förordningen 7 § om att kartlägga sina informationsprocesser.
- Den nya nationella styrmodellen (oklart innehåll som bedöms öka kostnader).
- Ökad resursåtgång för att bli en kvalificerad kravställare.
- Kravet på att använda certifierade och säkra produkter.
- Vidareutveckling, drift och förvaltning av de it-system som ska använda SGSI.
- Den nya obligatoriska incidentrapporteringen (oklart exakt hur).
- De nya obligatoriska sensorsystemen (oklart exakt hur).

Remissvaret har beslutats av generaldirektören Ingemar Hansson. Vid den slutliga handläggningen deltog även överdirektören Helena Dyrssen, avdelningschefen Marie Carlsson, enhetschefen Peter Sävje, säkerhetschefen Lotta Oscarsson, rättslige experten Gunnar Svensson och säkerhetsstrategen Roland Jidrot, föredragande.

Ingemar Hansson

Roland Jidrot