Polisen

Datum
2015-09-21

Diarienr (åberopas)	Saknr	Er referens
A212.060/2015	000	Ju2015/2650/SSK

Polismyndigheten
Rättsavdelningen

Justitiedepartementet
Enheten för samordning av samhällets krisberedskap (SSK)
103 33 Stockholm

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

Allmänt

Polismyndigheten är positiv till att det tas fram en förordning för statliga myndigheters informationssäkerhet och en strategi för informations- och cybersäkerhet i staten. Polismyndigheten instämmer i huvudsak med betänkandets förslag till åtgärder, men vill i några utvalda delar i betänkandet framföra synpunkter, se nedan.

Detta gäller bl.a. utredningens förslag om att införa en obligatorisk rapporteringsskyldighet till Myndigheten för samhällsskydd och beredskap (”MSB”) av it-incidenter som allvarligt kan påverka säkerheten i den informationshantering som en myndighet ansvarar för. Ur ett strikt polisärt perspektiv kan det enligt Polismyndighetens mening vara bättre med ett system för obligatorisk incidentrapportering som utformas på så sätt att allvarliga informationssäkerhetsincidenter som rör *misstanke om brott* och som inte omfattas av Säkerhetspolisens tillsynsområde istället rapporteras till Polisen som första mottagare, se avsnitt 9.5.2 nedan.

1.1 – Förslag till förordning för statliga myndigheters informationssäkerhet

Nedan lämnar Polismyndigheten konkreta förslag på ändringar och tillägg till utredningens författningsförslag.

Definitioner
4 §
För den rätta förståelsen av i förordningen förekommande begrepp är det viktigt att dessa begrepp definieras enligt vedertagen terminologi. Begrepp och definitioner som används i SIS standard TR 50 bör genomgående användas. I detta avseende finns anledning att påpeka att definitionen av ”informationssäkerhet” inte följer SIS TR 50. Enligt SIS TR 50 ingår inte ”spårbarhet” som en av de grundläggande aspekterna för informationssäkerhet. Spårbarhet är en skyddsåtgärd för att tillgodose krav på konfidentialitet, riktighet och tillgänglighet och ska följaktligen inte finnas med i denna uppräkning.

Vidare används i förordningen genomgående begrepp som ”it-incident”. Att rapportera it-incidenter kan leda till ett rapporteringsöverflöde då begreppet it-incident är för brett och felriktat. Begreppet it-incident är inte heller tillräckligt tydligt beskrivet. Polismyndigheten anser mot denna bakgrund att begreppet ”it-incident” i förordningen byts ut till ”informationssäkerhetsincident” då det är informationssäkerhet och inte it som är syftet med förordningen. Rapportering av informationssäkerhetsincidenter träffar fler relevanta områden som bör rapporteras än it-incidenter. Nu föreslagna justering ska gälla för 7, 10, 11, 15, 17 och 20 §§ i förordningen.

Polismyndigheten anser även att andra förekommande begrepp i förordningen närmare bör definieras. Här nedan ges förslag på begrepp med efterföljande definition:

”**informationssäkerhet** – förmågan att upprätthålla konfidentialitet, riktighet och tillgänglighet i sin informationshantering.”

”**ledningssystem** - grupp av samverkande eller varandra påverkande delar av en organisation för att upprätta policy och mål samt processer för att uppnå dessa mål.”

”**informationssäkerhetsincident** – enskild eller flera oönskade eller oväntade informationssäkerhetshändelser som har negativa konsekvenser för verksamheten och dess informationssäkerhet.”

”**säkerhetskultur** - gemensamma attityder, värderingar och uppfattningar som chefer och anställda har om förhållandet till säkerhet.”

Myndighetens informationssäkerhetsarbete

6 §
Sista stycket: Begreppet säkerhetskultur bör definieras.

7 §
Ordningen och beskrivningen av vilka åtgärder som ska göras följer inte en vedertagen ordning för hur detta regelmässigt brukar beskrivas.

Första stycket:

- Det är missvisande att ange att ”informationsprocesser” ska kartläggas.
- Sista ordet spårbarhet ska med hänvisning till SIS TR 50 inte ingå som en av de grundläggande aspekterna utan är endast en säkerhetsåtgärd som är en funktion till de övriga (se under 4 §). Vidare är kraven på konfidentialitet, riktighet, tillgänglighet definierade som ”informationssäkerhet” under 4 §.

Polismyndigheten föreslår mot denna bakgrund att första stycket ska få följande lydelse:
”Myndigheten ska kartlägga informationen i sin verksamhet och klassificera informationen med utgångspunkt i kravet på informationssäkerhet.”

Andra stycket: Begreppet ”it-incidenter” bör ändras till ”informationssäkerhetsincidenter”. Polismyndigheten anser även att det bör ställas ett utökat och tydligare krav på att myndigheten, utöver förmågan att kunna identifiera och hantera incidenter, även ska ha förmågan att kunna förebygga dessa.
Stycket bör vidare byta plats med nuvarande tredje stycke i denna paragraf.

Sista meningen i tredje stycket: Det är missvisande att ange att man ska följa utvecklade krav- och skyddsnivåer då dessa inte finns. Polismyndigheten föreslår att meningen istället ska få följande lydelse:
”I de fall krav- och skyddsnivåer för offentlig förvaltning finns utpekade i verkställighetsföreskrifter som meddelats med stöd av denna förordning ska dessa följas i detta arbete.”

8 §
Denna paragraf är svår att tolka och förstå. Begreppet säkra it-produkter bör definieras. Detta bör enligt Polismyndigheten lämpligen ske i de verkställighetsföreskrifter som MSB meddelar på området. I paragrafen ställs inga krav på tjänster vilket enligt Polismyndighetens uppfattning torde vara lika viktigt som krav på produkter (jfr 15-16 §§).

Första meningen: Det är också svårt att endast göra koppling till risk- och sårbarhetsanalyser för att få fram om man ska använda säkra it-produkter eller inte. Polismyndigheten anser att kopplingen även borde ske utifrån klassificeringen av information. Myndigheten föreslår således att första meningen ska få följande lydelse:
”Myndigheten ska, med stöd av informationsklassificeringen och risk- och sårbarhetsanalyser, välja och använda säkra it-produkter vid hantering av information…”

9 §
Första stycket: Utöver hänvisningen till 7-8 §§ borde hänvisning även ske till 5 §.

Första meningen i andra stycket. Kontinuitetsarbete syftar inte enbart till att upprätthålla förmåga att hantera sina uppgifter under fredstida krissituationer och höjd beredskap. Det kan vara mindre allvarliga situationer men det är ändå viktigt att myndigheten kan utföra sina uppgifter. Polismyndigheten föreslår mot denna bakgrund att första meningen i andra stycket ska få följande lydelse:
”Myndigheten ska med stöd av kontinuitetshantering upprätthålla en sådan nivå av informationssäkerhet att myndigheten har en god förmåga att hantera sina uppgifter.”

10 §
Enligt Polismyndighetens mening bör den ”anlitande myndigheten” vara ansvarig för sitt informationssäkerhetsarbete oavsett om informationshanteringen utförs av en annan myndighet eller ett privat bolag. Polismyndigheten föreslår mot denna bakgrund att första stycket ska få följande lydelse:

”Kraven i 5-9 §§ gäller endast i tillämpliga delar sådana myndigheter vars informationshantering eller vars informationssäkerhetsarbete administreras av en annan myndighet, en så kallad värdmyndighet, eller av annan extern part.
I de fall den anlitande myndigheten uppdragit åt en sådan värdmyndighet eller annan extern part att utföra informationshanteringen och/eller informationssäkerhetsarbetet ska den anlitande myndigheten tillse att informationssäkerhetsarbetet bedrivs enligt denna förordning.”

Andra stycket: Begreppet ”it-incidenter” bör ändras till ”informationssäkerhetsincidenter”.

Särskilda krav på informationssäkerhetsarbete

11 §
MSB har på vissa områden givits väl otydliga och långtgående mandat, inte minst enligt denna paragraf där MSB enligt den andra strecksatsen kan ställa särskilda krav på sensorsystem för it-incidentidentifiering. Polismyndigheten anser att det är svårt att ställa generella krav mot dessa myndigheter då det t.ex. för Polismyndigheten kan få negativa konsekvenser som måste analyseras.

Andra strecksatsen: Begreppet ”it-incidentidentifiering” bör ändras till ”informationssäkerhetsincidentidentifiering”.

Tredje strecksatsen: Kompetenskraven bör enligt Polismyndigheten kunna omfatta en bredare personkrets och inkludera dels informationssäkerhetschefen eller motsvarande person som ytterst ansvarar för informationssäkerhetsarbetet inom myndigheten samt dels de övriga personer som leder och samordnar det praktiska arbetet med informationssäkerhet (jfr 6 §).

Upphandling och utveckling av it-system och it-produkter

Polismyndigheten ställer sig frågande till varför minimikrav endast ställs vid upphandling av it-produkter, men inte vid upphandling av it-tjänster? Då utredningens förslag till det andra målet, att Staten blir en tydligare kravställare, omfattar såväl produkter som tjänster (se s.17 och avsnitt 9.1.4) borde 15-16 §§ även reglera minimikrav vid upphandling av tjänster.

15 §
Fjärde stycket: Begreppet ”it-incidenter” bör ändras till ”informationssäkerhetsincidenter”.

16 §
I sista delen i första meningen anges att endast ”säkra och certifierade it-produkter” ska användas. På andra områden i förordningen har krav endast omfattat ”säkra it-produkter”, se bl.a. i 8 §. Det bör utvecklas om syftet är att produkterna alltid ska vara certifierade.

Att en myndighet enbart ska använda sig av säkra och certifierade produkter för samhällsviktiga produkter och system kommer att leda till minskade valmöjligheter och ökade kostnader och komplexitet. Polismyndigheten anser att det under en övergångsperiod bör finnas möjlighet att använda sig av andra produkter.

It-incidentrapportering

I enlighet med det ovan framförda bör rubriken ha lydelsen ”Informationssäkerhetsincidentrapportering”.

17 §

Angående incidentrapporteringssystemet, se Polismyndighetens synpunkter under avsnitt 9.5.2 nedan.

Första stycket: Begreppet ”it-incidenter” bör ändras till ”informationssäkerhetsincidenter”.

I denna paragraf refereras vidare till en ny bestämmelse i 10 a § säkerhetsskyddsförordningen (1996:633) som syftar till att säkerställa att inträffade it-incidenter som allvarligt kan påverka säkerheten i ett informationssystem där hemliga uppgifter behandlas ska anmälas av den myndighet som berörs av incidenten till den myndighet som enligt 39 § nämnda förordning utövar tillsyn över säkerhetsskyddet. Det noteras att nämnda förordning för närvarande är föremål för omfattande översyn enligt betänkandet En ny säkerhetsskyddslag SOU 2015:25, vilket även kommer att påverka innehållet i denna paragraf.

Tillsyn, föreskrifter och myndighetsrådets uppgifter

En generell synpunkt är att 18-20 §§ lämpligen kan delas upp i tre underrubriker benämnda; Myndighetsrådet, Tillsyn och Verkställighetsföreskrifter.

18 §

Polismyndigheten anser att myndighetsrådets uppgifter är otydliga. De uppgifter som uppräknas i denna paragraf är en blandning mellan strategiska, taktiska och operativa uppgifter. Myndighetsrådet uppgifter borde enligt Polismyndighetens uppfattning ha en mer strategisk inriktning. De strategiska uppgifterna bör bl.a. innefatta att:

- utgöra en gemensam beredning- och remissinstans på informationssäkerhetsområdet.
- förvalta samhällets strategi för informations- och cybersäkerhet.
- bistå med expertkunskap till regeringen, MSB och övriga myndigheter (bl.a. i samband med upphandling av tjänster och produkter på informationssäkerhetsområdet, vid utveckling av tillämpliga krav och kontrollanordningar i standarder för produkter och tjänster med bäring på informationssäkerhet i samhällsviktig verksamhet, vid utveckling av krav- och skyddsnivåer samt i samband med MSB:s tillsyn).

Härigenom renodlas myndighetsrådets uppgifter och tydliggörs att rådet endast har en stödjande funktion till MSB som har till uppgift att utveckla de krav som ska gälla för statens informationssäkerhet.

19 §
Polismyndigheten är positiv till utredningens förslag att MSB ska utöva tillsyn över statliga myndigheters informationssäkerhetsarbete. Det noteras dock att tillsynsansvaret ska regleras i lag, inte i förordning.

Enligt Polismyndighetens mening kan det finnas problem med att blanda tillsynsuppgifterna med uppgifter som främjande och normering. Särskilt problematiskt är detta för främjandeuppgifter, som rådgivning och bidragsgivning, där det finns en stor risk att myndighetens opartiskhet kan ifrågasättas. Det är t.ex. inte lämpligt att tillsynsmyndigheten lämnar konkreta råd i enskilda fall. Att däremot redogöra för gällande lagstiftning eller ge mer allmänna råd och rekommendationer är vanligtvis inte problematiskt, utan kan snarare bidra till ett bra resultat av tillsynen. Det är därför viktigt att regeringen ser över vilka uppgifter MSB ska ha.

Då MSB har främjande och/eller normeringsuppgifter är det viktigt att dessa uppgifter organisatoriskt inom myndigheten skiljs från tillsynsuppgiften. Detta gäller främst för att undvika eventuella jävsituationer. En direkt olämplig främjandeuppgift för en tillsynsmyndighet är att reellt (inte bara formellt) besluta om olika typer av bidrag inom tillsynsområdet. Dessa bidrag kan även vara att stödja vissa projekt inom området hos en myndighet.

En annan viktig del att utreda vidare är om några sanktioner ska vara kopplade till tillsynsverksamheten vid en myndighets bristande efterlevnad av förordningen eller om detta ska lösas på annat sätt.

MSB måste även ha tillräckliga resurser och kompetens för att utföra uppgiften och för att klara händelsestyrd tillsyn efter incidenter.

20 §
Enligt Polismyndighetens uppfattning bör verkställighetsföreskrifter även kunna meddelas rörande tillsynen.

Fjärde punkten: Begreppet it-incidentrapportering bör ändras till ”informationssäkerhetsincidentrapportering”.

9.2.1 En nationell styrmodell

Det är positivt med en gemensam modell för att styra och kontrollera informationssäkerheten i svensk statsförvaltning. Polismyndigheten anser dock att denna styrmodell, förutom att baseras på existerande krav i författningar och verksamheternas behov även måste baseras på standarder inom området. Det är en förutsättning för att få en enhetlighet i hela samhället och inte bara inom statsförvaltningen. Det möjliggör dessutom enhetlighet och igenkänning även på den internationella arenan. Något som är nog så viktigt för stora delar av den offentliga förvaltningen.

Innebörden och innehållet i en nationell styrmodell behöver noga analyseras och diskuteras med ett flertal aktörer och experter på området. Det finns även en risk med att strukturera upp gemensamma arbetsmetoder med mera i för stor utsträckning. Behoven är till stor del desamma, men verksamheterna skiljer sig åt och därmed även behoven. Om det i dag kan vara problem att få till metoder som accepteras inom en myndighet därför att de olika verksamhetsdelarna anser att just deras behov inte tillgodoses tillräckligt så lär det bli svårt att göra detta på nationell nivå.

9.2.3 En ny förordning för statliga myndigheters informationssäkerhet

Polismyndighetens synpunkter på författningsförslaget framgår ovan, se avsnitt 1.1.

9.2.5 Informationssäkerhet som en del av myndighetens revision

Utan att egentligen beskriva varför, lyfter utredningen i detta avsnitt fram att uppföljning och revision av informationssäkerhet är ett område som bör utvecklas. Utredningen anger att det har konstaterats brister i arbetet med uppföljning och revision (sid 232) utan att presentera något underlag för denna bedömning. Utredningen anger vidare att det särskilt är reglerna för intern revision som upplevs uppvisa brister.

Polismyndighetens anser att det finns otydligheter i hur utredningen använder begreppet revision och det är oklart vad det är som avses. Olika ord används, exempelvis säkerhetsrevision (sid 53), intern revision (sid 235) och internrevision (sid 235). Begreppen uppföljning och revision används i stor utsträckning som ett samlat begrepp utan att det framgår om man menar två olika saker (vilket det är) eller om man ser det som ett sammanhang.

Det finns olika betydelser i begreppet revision beroende på dess syfte/uppdrag. Exempel på olika typer av revision är: internrevision, miljörevision, externrevision, interna revisioner enligt ISO- 27000-familjen. Det finns således två olika sorters intern revision (internrevision och intern revision):

- internrevision utifrån internrevisionsförordningen (2006:1228)
- interna revisioner och granskningar som beskrivs i ISO-27000-familjen.

Internrevisionsförordningen och IIA:s standards innebär att internrevisionen ska omfatta all verksamhet som myndigheten bedriver eller ansvarar för. Internrevisionens uppdrag är att granska ledningens interna styrning och kontroll utifrån kraven i 3 § myndighetsförordningen (2007:515). Urval av revisionsuppdrag sker med utgångspunkt från en analys av verksamhetens risker som t.ex. skulle kunna vara informationssäkerhet.

I ISO-27000-familjen finns begreppen interna revisioner och granskningar. I 27001 används interna revisioner och syftet är att dessa ska genomföras med planerade intervall för att säkerställa att alla delar i standarden är uppfyllda. I 27002 används begreppen granskningar och oberoende granskningar med syfte

att säkerställa att informationssäkerhet införs och drivs i enlighet med organisationens regler och rutiner. Här krävs detaljerad sakkunskap inom informationssäkerhetsområdet hos den funktion som ska utföra granskningarna. Den interna revision som ISO 27000-familjen avser är således en del i ledningssystemet.

För organisationer finns en allmänt accepterad modell som innehåller tre ansvarsnivåer.

1. Första ansvarsnivån utför myndighetens dagliga löpande verksamhet. Denna ansvarslinje äger, hanterar sina risker och kontroller.
2. Andra ansvarslinjen utgörs av myndighetens egna uppföljningar och kontroller. Avser arbetsuppgifter som utförs av chefer, controllers, särskilda funktioner för regelefterlevnad, risk samt ”interna revisioner” av miljö-, informations- och kvalitetsledningssystem.
3. Tredje ansvarsnivån utgörs av internrevisionen. Internrevisionen har ingen del i myndighetens dagliga arbete, uppföljning eller kontroller utan ska vara oberoende vilket innebär att man inte deltar i uppgifter som utförs på första och andra ansvarsnivån. Internrevisionen ska istället bedöma om de två första ansvarslinjerna har fungerat som det var tänkt, att intern styrning och kontroll är betryggande.

Polismyndigheten instämmer i att det finns ett behov av att förstärka den interna styrningen och kontrollen för informationssäkerhetsområdet. Enligt Polismyndighetens uppfattning bör det ske genom ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av ett ledningssystem. Utredningen drar slutsatsen att de brister som har identifierats i huvudsak har orsakats av bristande uppföljning och revision. Enligt Polismyndighetens uppfattning beror de identifierade bristerna till stora delar på att något ledningssystem för informationssäkerhet inte har implementerats eller brister i implementering av föreskriftens krav. En väl fungerande process för informationssäkerhet kännetecknas av att det finns en struktur för god intern styrning och kontroll. Det bidrar till att informationssäkerhetsarbetet bedrivs effektivt och med god ekonomisk hushållning, såsom det kommer till uttryck i verksamhetskraven i myndighetsförordningen. Om myndigheten implementerat MSB:s föreskrifter som bygger på standarden (27001, 27002) skapas en bra struktur för att uppnå en god intern styrning och kontroll. Enligt Polismyndigheten kommer mer uppföljning och revision inte leda till några större förbättringar om det inte finns någon implementerad struktur för den interna styrningen och kontrollen.

Enligt Polismyndighetens mening finns det inga brister i reglerna för intern revision (om man med detta menar internrevision enligt internrevisionsförordningen) vad avser informationssäkerhetsområdet. Interrevisionen kan redan idag granska området informationssäkerhet under förutsättning att man har bedömt att det finns risker inom området. Dock är det oklart vilken sorts revision som utredningen syftar på. Polismyndigheten får intrycket av att det som utredningen i huvudsak efterlyser när de anger intern revision egentligen är

uppföljning enligt andra ansvarsnivån enligt ovan. Polismyndigheten anser att det vore olyckligt om internrevisionen ålades ett årligt återkommande arbete för att lämna ett uttalande om myndighetens informationssäkerhet i årsredovisningen, då detta dels strider det mot intentionerna i internrevisionsförordningen, dels mot principerna om tre ansvarsnivåer i myndigheten. Om ett rapporteringskrav införs i årsredovisningen bör ansvaret för granskning av denna tilldelas andra ansvarsnivån i organisationen. Genom ett sådant eventuellt införande kommer rapporteringen även att bli föremål för extern revision.

9.5.2 Obligatorisk it-incidentrapportering

Polismyndighet delar utredningens uppfattning att samhällets informationssäkerhetsarbete är mycket viktigt och bör prioriteras. Polismyndigheten är även positiv till att det införs ett system för obligatorisk rapportering av informationssäkerhetsincidenter för alla statliga myndigheter. Detta är i grunden en bra målsättning.

Utifrån ett polisiärt perspektiv finns det emellertid aspekter som talar för att Polismyndigheten bör vara första mottagare av vissa incidenter. Som nämns i betänkandet har de brottsbekämpande myndigheterna befogenhet och skyldighet att uppdaga, beivra och utreda brott i den digitala miljön (se avsnitt 9.6). Polisens uppdrag framgår av polislagen och polisförordningen. Regeringen har i budgetpropositionen 2011/12, sid 90, angående behovet av en obligatorisk incidentrapportering uttalat att ”..även Rikspolisstyrelsen (RPS) (kan) ha behov av it-incidentrapportering” samt att ”..en it-incident som innefattar en brottslig handling faller inom polisens ansvarsområde”. För att Polismyndigheten ska kunna uppdaga brotten är det utifrån en polisiär utgångspunkt viktigt att Polismyndigheten får relevant information om allvarliga incidenter av brottslig karaktär.

En stor del av de allvarliga informationssäkerhetsincidenter som MSB kommer att få kännedom om kommer sannolikt utgöra brott. Detta får till följd att MSB får kännedom om brott mot statliga myndigheter utan krav eller, p.g.a. sekretesshinder, möjlighet att överlämna uppgifterna till Polisen för utredning och lagföring. Utifrån en polisiär utgångspunkt är det viktigt att Polismyndigheten i ett inledande skede får vetskap om dessa informationssäkerhetsincidenter för att kunna bedöma om brott föreligger.

En lägesbild som visar den faktiska brottsligheten underlättar arbetet med att bekämpa it-relaterad brottslighet och särskilt gällande angrepp mot kritisk infrastruktur. Detta förutsätter att Polisen har tillgång till information om allvarliga incidenter. Vid ett medvetet antagonistiskt angrepp är det en brottsutredande myndighet som ska hantera ärendet. Om det inte är ett ärende för Säkerhetspolisen så bör Polismyndigheten vara mottagare när det gäller allvarliga informationssäkerhetsincidenter av brottslig karaktär.

It-brott har även särdrag som gör att det är det ur polisiär utgångspunkt är viktigt att Polisen är första mottagare av incidenter för att kunna vidta adekvata initiala åtgärder, t.ex. avseende användandet av kvalificerade tvångsmedel. Tidsfaktorn är ofta avgörande i dessa ärenden. Uppgifter rörande incidenten finns ofta hos flera aktörer och det är tidskritiskt att säkra bevis hos dessa.

Tvångsåtgärder till säkerställande av detta måste ske enligt gällande lagstiftning och med beaktande av integritets- och sekretessfrågor. Möjlighet att vidta dessa åtgärder har endast Polisen. En angripare kan befinna sig var som helst i världen och det är avgörande att komma igång snabbt med brottsutredande åtgärder såsom t.ex. spårningar och begäran om rättshjälp. Även det internationella polissamarbetet är av stor betydelse i dessa ärenden och nationella operativa avdelningen (NOA), som utgör nationell kontaktpunkt i internationell polissamverkan, har ett mycket väl fungerande och upparbetat polisiärt samarbete.

En konsekvens av att Polisen inte får tillgång till information i direkt anslutning till att det skett en allvarlig informationssäkerhetsincident av brottslig karaktär kan ur ett polisiärt perspektiv bli att Polisen inte klarar av att utreda dessa brott. En annan konsekvens kan bli att Polisen inte kan delge relevant information och kunskap inom området till MSB, Säkerhetspolisen eller andra internationella partners. Detta kan i viss mån sägas innebära en motsatsställning mot utredningens mål att stärka det förebyggande arbetet och bekämpandet av it-relaterad brottslighet (avsnitt 9.6) och att Sverige ska vara en stark internationell partner (avsnitt 9.7).

Ur ett strikt polisärt perspektiv kan det således vara bättre med ett system för obligatorisk incidentrapportering som utformas på så sätt att allvarliga informationssäkerhetsincidenter som rör *misstanke om brott* och som inte omfattas av Säkerhetspolisens tillsynsområde istället rapporteras till Polisen som första mottagare. Ett sådant system torde i förlängningen kunna ge Polisen bättre förutsättningar att nå en högre uppklarningsfrekvens av ingångna brott. I ett sådant system är det viktigt med klara gränssnitt mellan ”misstänkta brott” och ”icke brott” så att MSB och Polismyndigheten kan fullgöra sina respektive uppdrag. För Polisens del handlar det både om det brottsförebyggande arbetet och arbetet med att utreda och beivra brott.

En jämförelse kan i detta hänseende göras med det rapporteringskrav som gäller för verksamhetsutövare på den finansiella marknaden enligt lagen (2009:62) om åtgärder mot penningtvätt och finansiering av terrorism. Enligt nämnda lag åligger det verksamhetsutövaren att utan dröjsmål rapportera alla omständigheter som kan tyda på penningtvätt eller finansiering av terrorism till Polismyndigheten. Penningtvättsanmälningar är underrättelseinformation och omfattas av sekretess. Uppgifterna kan därefter bli underlag till underrättelserapporter som överlämnas till den utredande verksamheten för att ligga till grund för att inleda en förundersökning. Polismyndigheten anser att det inte går att utesluta att även informationssäkerhetsincidenter kan utgöra en del av en terrorattack.

Polisen har redan idag en upparbetad verksamhet där it-incidenter utreds på såväl nationell som internationell nivå. Dessutom finns det ett beslut om att ett nationellt it-brottscentrum ska inrättas vid Polismyndigheten. Syftet med centrumet är att leva upp till de krav som det europeiska it-brottscentrumet, European cyber crime center, ställer på medlemsstaterna. Förslagsvis kan det nationella it-brottscentrumet bli ingångskanal för dessa informationssäkerhetsincidentrapporter.

En fungerande myndighetssamverkan finns idag inom andra prioriterade områden t.ex. satsningen mot grov organiserad brottslighet. En liknande lösning torde med lite god vilja gå att åstadkomma även inom detta prioriterade område. Även åklagarmyndigheten bör bjudas in till fortsatta diskussioner eftersom det ofta handlar om att redan under pågående förundersökning få till en nära samverkan mellan myndigheterna.

Mot detta står utredningens förslag om att den obligatoriska it-incidentrapporteringen ska ske till MSB. Polismyndigheten ser naturligtvis fördelarna med ett sådant system utifrån ett samhälleligt perspektiv. Härigenom kan kunskapen om hur många incidenter som inträffar och omfattningen av dessa samlas på ett ställe, en myndighet. Denna kunskap kan vara värdefull för att förstärka samhällets förmåga att förebygga och hantera incidenter som hotar eller skadar samhällsviktig verksamhet. Utifrån detta perspektiv och baserat på de skäl som utredningen anger kan det vara rimligt att MSB anförtros uppgiften att ta emot de it-incidentrapporter som lämnas från myndigheterna. MSB är den myndighet som enligt sin myndighetsinstruktion[1] för närvarande ansvarar för it-incidenthanteringen. Det kan därför förefalla naturligt att MSB även fortsättningsvis får detta uppdrag.

Om regeringen skulle komma fram till att myndigheterna ska fullgöra rapporteringsskyldigheten endast till MSB i enlighet med utredningens förslag, bör det åvila MSB att rekommendera berörda myndigheter att även skyndsamt rapportera inträffade informationssäkerhetsincidenter av brottslig karaktär till Polismyndigheten. Detta bör kunna ske genom ett förtydligande i 17 § i den föreslagna förordningen för statliga myndigheters informationssäkerhet. I detta sammanhang vill Polismyndigheten särskilt påtala vikten av att systemet, som utredningen antyder, …”bör utformas så att det säkerställer behovet hos de brottsbekämpande myndigheterna av att kunna informera sig om misstänkta brottsliga angrepp” (sid 261). I det fall den rapporteringsskyldige myndigheten redan har polisanmält en incident föreslår Polismyndigheten att ett mer begränsat rapporteringskrav till MSB införs, där krav på rapportering endast omfattar uppgift om att en informationssäkerhetsincident har inträffat, vem som har drabbats och att incidenten har polisanmälts. På detta sätt kan inte uppgifterna komma att motverka en pågående förundersökning eller annan brottsförebyggande verksamhet. Detta bör kunna komma till uttryck i MSB:s verkställighetsföreskifter på området.

Enligt Polismyndighetens mening är valet mellan MSB, å ena sidan, och Polismyndigheten, å andra sidan, som mottagare av informationssäkerhetsincidentrapporter av nu angivet slag ytterst en fråga som kräver ett politiskt ställningstagande. Polismyndigheten överlämnar till regeringen att välja inriktning.

[1] Se 11 a § förordningen (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap

9.6.1 It-brottskonventionen

Polismyndigheten är positiv till utredningens mål att förebygga och bekämpa it-relaterad brottslighet. De förslag som nämns är viktiga för Polisens arbete att på ett effektivt och rättsäkert sätt kunna bekämpa denna brottslighet. Myndigheten delar således utredningens ståndpunkt att arbetet med att ratificera it-brottskonventionen snarast slutförs.

9.6.2 Informationsutbyte

Polismyndigheten instämmer i utredningens bedömning att det bör utredas om en tydligare reglering kan införas i offentlighets- och sekretesslagen (2009:400) rörande sekretess för uppgifter som utbyts i samverkan mellan brottsbekämpande myndigheter och andra myndigheter inom informationssäkerhetsområdet. Av de skäl som anges i utredningen är det enligt Polismyndighetens uppfattning mycket angeläget att denna fråga utreds.

9.6.3 Översyn av bestämmelser om tvångsmedel i den digitala miljön

Polismyndigheten välkomnar utredningens förslag till förnyad utredning, Tvångsmedel i den digitala miljön, med uppgift att se över bestämmelserna om tvångsmedel i 27 och 28 kap. rättegångsbalken samt övriga befintliga tvångsmedel avseende dess tillämpning i den digitala miljön. Såsom utredningen anger är de existerande tvångsmedlen inte anpassade för den digitala miljön, vilket leder till osäkerhet kring hur de kan, får och ska användas i denna miljö. Som utredningen antyder kan listan med exempel på denna typ av problem göras omfattande. Som ett exempel kan nämnas användandet av domännamn och webbsidor i brottsligt syfte. Inom detta område är angeläget att utreda vilka tvångsmedel som Åklagarmyndigheten och Polismyndigheten kan använda sig av.

10.2 Konsekvensanalys av åtgärdsförslagen

När det gäller konsekvensanalysen så delar Polismyndigheten uppfattningen att vissa av förslagen kan rymmas inom myndigheternas befintliga budget. Polismyndigheten vill emellertid framhålla att denna samlade ambitionshöjning ofrånkomligen kommer att medföra ett ökat resursbehov för de enskilda myndigheterna (även om behovet blir störst hos MBS).

Polismyndigheten vill också betona det utökade behovet av praktiskt stöd som förslagen medför, som inte får underskattas.

POLISMYNDIGHETEN

Eva Lindeblad
Chef för enheten för rättslig styrning och stöd

Per Luthander
Jurist och föredragande

Kopia till

Justitiedepartementet, PO
Arbetstagarorganisationerna
Rikspolischefens kansli