Nationell strategi för samhällets informations- och cybersäkerhet

Skr. 2016/17:213

Bilaga:
Uppdatering om genomförandet av Nationell strategi för samhällets informations- och cybersäkerhet

Regeringskansliet
Justitiedepartementet

Foto omslag: iStockphoto

Regeringens skrivelse 2016/17:213

Nationell strategi för samhällets informations- och cybersäkerhet

Skr. 2016/17:213

Regeringen överlämnar denna skrivelse till riksdagen.

Stockholm den 22 juni 2017

Morgan Johansson

Anders Ygeman
(Justitiedepartementet)

Skrivelsens huvudsakliga innehåll

Det finns ett stort behov av att utveckla samhällets informations- och cybersäkerhet. Denna nationella strategi för samhällets informations- och cybersäkerhet är ett uttryck för regeringens övergripande prioriteringar och syftar till att utgöra en plattform för Sveriges fortsatta utvecklingsarbete inom området. Huvudsyftena med strategin är att bidra till att skapa långsiktiga förutsättningar för samhällets aktörer att arbeta effektivt med informations- och cybersäkerhet samt att höja medvetenheten och kunskapen i hela samhället. Regeringen vill genom strategin även stödja de insatser och det engagemang som redan finns i samhället för att stärka informations- och cybersäkerheten. Strategin omfattar därmed hela samhället, det vill säga statliga myndigheter, kommuner och landsting, företag, organisationer och privatpersoner.

Innehållsförteckning

1 En samlad strategi för samhällets informations- och cybersäkerhet 5
1.1 Behovet av en strategi 5
1.2 Utgångspunkter för Sveriges informations- och cybersäkerhet....6

2 Strategiska prioriteringar....11
2.1 Säkerställa en systematisk och samlad ansats i arbetet med informations- och cybersäkerhet....11
2.2 Öka säkerheten i nätverk, produkter och system 16
2.3 Stärka förmågan att förebygga, upptäcka och hantera cyberattacker och andra it-incidenter 21
2.4 Öka möjligheterna att förebygga och bekämpa it-relaterad brottslighet....23
2.5 Öka kunskapen och främja kompetensutvecklingen 27
2.6 Stärka det internationella samarbetet....30

3 Uppföljning av strategin 35

Utdrag ur protokoll vid regeringssammanträde den 22 juni 2017....36

1 En samlad strategi för samhällets informations- och cybersäkerhet

1.1 Behovet av en strategi

Digitaliseringen är ett globalt fenomen och påverkar i stort sett alla delar av vårt samhälle. Det medför stora möjligheter, men också risker. Hur vi hanterar riskerna som följer av digitaliseringen har stor betydelse för vår förmåga att upprätthålla och stärka både vårt välstånd och vår säkerhet.

Informations- och cybersäkerhet är idag en fråga som angår hela samhället. Alla behöver ta sitt ansvar för informations- och cybersäkerhetsfrågor för att vi ska uppnå en effektiv och säker hantering av information. Ingen kan ensam lösa säkerhetsutmaningarna och när det är många olika aktörer som arbetar på olika sätt och i olika sammanhang är det särskilt viktigt med samverkan och en gemensam riktning. Behovet av samverkan mellan den offentliga sektorn och näringslivet växer särskilt i betydelse. Den tekniska utvecklingen är i allt väsentligt styrd av privata aktörer på marknaden och privata aktörer äger och driver också stora delar av den samhällsviktiga verksamheten.

Utmaningarna inom informations- och cybersäkerhetsområdet delas med andra länder. De strategiska lösningarna måste därför även utvecklas genom internationell samverkan och dialog kring förebyggande åtgärder, både inom EU och i andra internationella organ.

Kraven på samhällets informations- och cybersäkerhet ökar i allt snabbare takt. Utvecklingen och den förändrade användningen av ny teknik och nya innovationer innebär att hot blir svårare att upptäcka, att riskerna blir mer svårbedömda och att beroenden blir svårare att överskåda. De regelverksförändringar som nu genomförs både nationellt och inom EU är ett sätt att höja säkerhetskraven samt stärka formerna och strukturerna för det samlade informations- och cybersäkerhetsarbetet.

Digitaliseringen är en av vår tids största förändringar och den snabba utvecklingen av informations- och kommunikationsteknologi har stor inverkan på vår framtid. Sverige ligger långt framme i teknikutvecklingen. Den pågående utbyggnaden av fibernäten och ökad mobiltäckning uppgraderar de elektroniska kommunikationsnäten. Den digitala utvecklingen kan därmed i allt högre grad bidra till sysselsättning, innovation, effektivitet och tillväxt i Sverige.

Genom ett strukturerat och riskbaserat arbete med informations- och cybersäkerhet kan vi säkerställa den fortsatta digitaliseringen av samhället, samtidigt som vi också hävdar Sveriges säkerhet och nationella intressen såsom mänskliga fri- och rättigheter och samhällets funktionalitet. Ett strukturerat och riskbaserat arbete med informations- och cybersäkerhet är också en viktig förutsättning för svensk tillväxt och konkurrenskraft, och en nödvändighet för att näringslivet ska kunna

utveckla och tillhandahålla konkurrenskraftiga varor och tjänster. För att höja informations- och cybersäkerheten finns det ett behov av att alla berörda parter i högre grad samverkar mot gemensamma målsättningar.

Mot denna bakgrund har regeringen beslutat att ta fram en nationell strategi för samhällets informations- och cybersäkerhet. Strategin är ett uttryck för regeringens övergripande prioriteringar och syftar till att utgöra en plattform för Sveriges fortsatta utvecklingsarbete inom området. Huvudsyftena med strategin är att bidra till att skapa långsiktiga förutsättningar för samhällets aktörer att arbeta effektivt med informations- och cybersäkerhet samt att höja medvetenheten och kunskapen i hela samhället. Regeringen vill genom strategin även stödja de insatser och det engagemang som redan finns i samhället för att stärka informations- och cybersäkerheten. Strategin omfattar därmed hela samhället, det vill säga statliga myndigheter, kommuner och landsting, företag, organisationer och privatpersoner.

Med informations- och cybersäkerhet avses i denna skrivelse en uppsättning säkerhetsåtgärder för bevarande av konfidentialitet, riktighet och tillgänglighet hos information. Med konfidentialitet avses att obehöriga inte ska kunna ta del av informationen. Med riktighet menas att informationen inte förändras, manipuleras eller förstörs på ett obehörigt sätt. Med tillgänglighet menas att behöriga ska kunna ha tillgång till informationen på det sätt och vid den tidpunkt som tjänsterna erbjuder. För informationssäkerhet som avser digital information används i denna skrivelse även begreppet cybersäkerhet. I denna skrivelse används begreppen beroende av sitt sammanhang, där exempelvis cybersäkerhetsbegreppet är vanligt förekommande i en internationell kontext.

1.2 Utgångspunkter för Sveriges informations- och cybersäkerhet

Informations- och cybersäkerhetsarbete är nödvändigt för att samhället ska kunna fungera och utvecklas i linje med de mål som finns inom olika politikområden. Digitaliseringen innebär att en allt större andel av alla aktiviteter i samhället i olika grad är beroende av nätverk och informationssystem och därmed av informations- och cybersäkerhet.

Strategin för samhällets informations- och cybersäkerhet har sin utgångspunkt i målen för Sveriges säkerhet: att värna befolkningens liv och hälsa, liksom samhällets funktionalitet, samt förmågan att upprätthålla grundläggande värden som demokrati, rättssäkerhet och mänskliga fri- och rättigheter (prop. 2008/09:140, bet. 2008/09:FöU10, rskr. 2008/09:292). Strategin har även sin utgångspunkt i det it-politiska målet att Sverige ska vara bäst i världen på att använda digitaliseringens möjligheter (prop. 2011/12:1, bet. 2011/12:TU1, rskr. 2011/12:87).

Strategin för samhällets informations- och cybersäkerhet bygger på och konkretiserar de inriktningar för informations- och cybersäkerheten som regeringen anger i den nationella säkerhetsstrategin och i digitaliseringsstrategin (N2017/03643/D).

Den nationella säkerhetsstrategin anger att Sverige aktivt ska värna våra nationella intressen och försvara dem närhelst de riskerar att undermineras, inklusive mot de hot och risker som finns på det informationsteknologiska området.

Digitaliseringsstrategin anger att förutsättningarna i Sverige ska vara de bästa för alla att på ett säkert sätt ta del av, ta ansvar för samt ha tillit till det digitala samhället.

I dag finns bestämmelser om informationssäkerhet i olika regelverk. Informationssäkerhet är en av tre grundläggande säkerhetsskyddsåtgärder enligt säkerhetsskyddslagen (1996:627). Lagstiftningen gäller för de mest skyddsvärda verksamheterna i samhället och innebär långtgående krav på olika skyddsåtgärder. För övriga statliga myndigheter gäller de krav på informationssäkerheten som framgår av förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap. Bestämmelser om informationssäkerhet finns även i arkivlagen (1990:782), personuppgiftslagen (1998:204) och lagen (2003:389) om elektronisk kommunikation. Utöver dessa författningar finns myndighetsföreskrifter som reglerar informationssäkerhet inom ett flertal sektorer.

Flera författningar som reglerar informationssäkerhet kommer att förändras eller tillkomma inom de kommande åren. Det pågår för närvarande en översyn av säkerhetsskyddslagstiftningen med förslag om att bl.a. utvidga lagens tillämpningsområde för att uppnå ett bättre skydd för Sveriges säkerhet (SOU 2015:25). Europaparlamentets och rådets direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (NIS-direktivet), som ska vara genomfört i svensk lagstiftning senast maj 2018, anger bl.a. en skyldighet för alla medlemsstater att anta en nationell strategi för säkerhet i nätverk och informationssystem. En annan EU-lagstiftning, Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), kommer att börja tillämpas i maj 2018 och innebär högre krav på hanteringen av personuppgifter.

Flera utredningar och granskningar inom informations- och cybersäkerhetsområdet har de senaste åren pekat på brister i förhållande till dagens hot och risker. Bl.a. har Riksrevisionen granskat informationssäkerheten i statsförvaltningen (RIR 2016:8, RIR 2014:23). Även betänkandet Informations- och cybersäkerhet i Sverige innehåller ett flertal förslag på informations- och cybersäkerhetsområdet (SOU 2015:23). I den försvarspolitiska inriktningspropositionen bedömde regeringen att Sveriges samlade förmåga att förebygga, motverka och aktivt hantera konsekvenser av civila och militära hot, händelser, attacker och angrepp i cybermiljön måste utvecklas och förstärkas (prop. 2014/15:109).

Vad ska skyddas?

Det öppna demokratiska samhället är beroende av att önskad konfidentialitet, riktighet och tillgänglighet kan upprätthållas när man hanterar information. Det innebär att både informationen i sig och de system som används för att förvara och överföra informationen måste skyddas. Informations- och cybersäkerhetsarbete är en nödvändig verksamhet för att värna kvaliteten och effektiviteten hos samhällets funktioner och en förutsättning för att digitaliseringens möjligheter ska kunna tas tillvara. Sådana möjligheter handlar om allt från utvecklade digitala offentliga tjänster till uppkopplade och automatiserade fordon och fabriker. Ytterst handlar informations- och cybersäkerhet om att slå vakt om grundläggande värden och mål i samhället, som demokrati, mänskliga fri- och rättigheter, Sveriges frihet, säkerhet och rätt till självbestämmande samt tillväxt och ekonomisk stabilitet.

För att individer ska kunna tillvarata och utöva sina fri- och rättigheter behövs tillgång till riktig och lättillgänglig information. Detta är en förutsättning för att man ska kunna fatta välunderbyggda beslut och höjer kvaliteten och effektiviteten för alla typer av verksamheter och kontakter i samhället.

Viss informationen i samhället är känslig och behöver därför skyddas. Om känslig information förloras, stjäls, manipuleras eller sprids till obehöriga kan det få allvarliga följder. Det finns stora mängder information som är av avgörande betydelse för samhällets funktionalitet eller som innehåller integritetskänsliga uppgifter. Andra exempel på känslig information har att göra med brottsbekämpning, tekniska produkter, affärsförhållanden, totalförsvaret eller förhållanden som gäller andra stater.

I dag bygger systemen för att hantera information huvudsakligen på digital informations- och kommunikationsteknologi. Detta gäller inte minst de system Sverige är beroende av för att kunna styra och leda riket under omfattande påfrestningar som kan följa av kris eller krig. Sådana system måste säkras. Vidare bygger många verksamheter i samhället på fungerande digitala informations- och styrsystem vilket innebär att stora mängder känslig information kontinuerligt hanteras i syfte att styra t.ex. eldistribution, vattenförsörjning, transporter och transportinfrastruktur eller sjukhusutrustning. Även industriella verksamheter inom t.ex. verkstadsindustri som processindustri är i dag beroende av fungerande digitala informations- och styrsystem. Incidenter hos och angrepp mot svenskt näringsliv kan få långtgående konsekvenser för enskilda företag såväl som för hela värdekedjor, och därmed hota svenska arbetstillfällen.

Beroenden och kopplingar mellan olika tekniska system är en sårbarhetsfaktor i sig genom att störningar kan få konsekvenser som är svåra att förutse och hantera. Detta gäller inte minst då de flesta nätverk och informationssystem är globalt sammankopplade via internet. Internet är i dag en global infrastruktur och det svenska samhällets kritiska infrastruktur är i hög grad integrerat med internet. Internet är så väsentligt att ett angrepp mot eller andra incidenter inom denna infrastruktur kan leda till allvarliga konsekvenser för Sveriges säkerhet och nationella intressen.

Hot- och riskskalan inom det informationsteknologiska området spänner från mindre omfattande risker för den enskilde individen till väl planerade och med precision riktade angrepp mot vitala delar av samhällets funktionalitet. Olika former av störningar i mjuk- eller hårdvara eller störningar i driftmiljö är vanligt förekommande. Yttre fysiska händelser som t.ex. bränder, avgrävda kablar, översvämningar eller solstormar utgör också en del av hotbilden.

I princip alla, såväl privatpersoner som näringsliv och offentlig verksamhet, som är anslutna mot internet är i dagsläget utsatta för risker eftersom det ständigt pågår intrångsförsök mot internetanslutna system. Den här typen av massangrepp är ofta mer eller mindre slumpartade. Ett exempel på detta är den stora ökningen av bedrägerier och identitetsstölder som sker via internet. Enligt Brottsförebyggande rådet (Brå) visar statistik att brottslighet med it-inslag (datorbedrägeri, bedrägeri med hjälp av internet, dataintrång samt internetrelaterade barnpornografibrott) har ökat med 949 procent mellan 2006 och 2015 (2016:17). Den som ansvarar för ett it-system måste utgå från att intrång och attacker kan lyckas, trots att en stor mängd faktiskt avvärjs. Riktade intrång och attacker kan utföras av enskilda individer, grupper av individer, icke-statliga organiserade grupper eller stater och statsunderstödda aktörer.

Det möjliga agerandet av stater, statsunderstödda aktörer eller andra aktörer med liknande förmåga utgör det allvarligaste informations- och cybersäkerhetshotet mot Sverige. Dessa kvalificerade angripare har förmåga, resurser och uthållighet att utarbeta och använda avancerade metoder. Cyberattacker och olika former av intrång i it-system kan utgöra ett separat antagonistiskt hot såväl som ett av flera politiska och militära maktmedel. Spionage och angrepp från statliga och statsunderstödda aktörer mot skyddsvärd verksamhet i Sverige eller mot svenska intressen i utlandet kan exempelvis syfta till att tillskansa sig information om svenska ekonomiska intressen, svenska företag, svensk forskning, svensk försvarsförmåga och planering, våra säkerhetspolitiska avsikter, samhällsviktig verksamhet och kritisk infrastruktur.

Dolda intrång och attacker kan användas i syfte att förbereda för sabotage mot kritisk infrastruktur i fredstid. Det kan också användas öppet som ett verktyg under främst inledande skeden vid militära insatser. Cyberattacker kan få stora konsekvenser för samhällsviktiga funktioner och kritiska it-system på samma sätt som ett konventionellt väpnat angrepp och kan därför i vissa fall vara att betrakta som ett väpnat angrepp.

Angrepp kan även riktas mot våra grundläggande värden och de demokratiska funktionerna i samhället, t.ex. genom desinformation och påverkanskampanjer. Desinformation kan användas för att avsiktligt sprida osanna eller vilseledande uppgifter i syfte att påverka människors attityder, ställningstaganden och handlande i en viss riktning. En påverkanskampanj är centralt styrd samtidigt som ett brett spektrum av metoder kan användas, såväl öppna som dolda, varav dataintrång och andra cyberattacker kan utgöra en delmängd. Den kan också inkludera politiska, diplomatiska, ekonomiska och militära maktmedel. Spridande

av oriktig eller vilseledande information riskerar att undergräva förtroendet för våra offentliga institutioner och utmana samhällets säkerhet. Källkritik och tillgång till en mångfald av oberoende medier och nyhetsförmedling stärker medvetenheten och motverkar effekterna av desinformation och påverkanskampanjer.

Antalet cyberattacker med syfte att påverka medier förväntas öka. Det handlar exempelvis om att genom överbelastningsattacker hindra tillgång till medierna men även om mer avancerade attacker i syfte att genom dataintrång stjäla information eller kapa webbplatser eller sändningar för att föra in falsk eller vilseledande information.

Hur skyddar vi oss?

Arbetet med att skydda oss är ett ansvar för hela samhället. Arbetet bedrivs hos såväl regeringen som i den egna verksamheten hos kommuner, landsting, myndigheter, företag och organisationer i Sverige. Ett systematiskt informationssäkerhetsarbete är nödvändigt för att samhällets aktörer ska kunna upprätthålla en väl avvägd nivå av informations- och cybersäkerhet – allt i samhället kan inte skyddas mot alla typer av hot och risker. Den tekniska säkerheten behöver fortsatt stärkas samtidigt som hänsyn tas till att det i många fall är den mänskliga faktorn som ligger bakom incidenter eller utnyttjas vid angrepp. Av den anledningen är det viktigt att öka medvetenheten såväl som förmågan hos alla användare av it-system och att skapa förutsättningar för utvecklingen av en säkerhetskultur i hela samhället.

För att sårbarheter ska minska och för att målen för Sveriges säkerhet och it-politik ska kunna främjas är det regeringens bedömning att arbetet med samhällets informations- och cybersäkerhet framförallt behöver prioritera att

– säkerställa en systematisk och samlad ansats i arbetet med informations- och cybersäkerhet
– öka säkerheten i nätverk, produkter och system
– stärka förmågan att förebygga, upptäcka och hantera cyberattacker och andra it-incidenter
– öka möjligheterna att förebygga och bekämpa it-relaterad brottslighet
– öka kunskapen och främja kompetensutvecklingen
– stärka det internationella samarbetet.

För var och en av dessa prioriteringar ställer regeringen i följande avsnitt upp ett antal målsättningar och anger en inriktning för hur målsättningarna ska nås.

2 Strategiska prioriteringar

2.1 Säkerställa en systematisk och samlad ansats i arbetet med informations- och cybersäkerhet

Systematiskt informationssäkerhetsarbete

Målsättningar:
- Statliga myndigheter, kommuner, landsting, företag och andra organisationer ska ha kännedom om hot och risker, ta ansvar för sin informationssäkerhet och bedriva ett systematiskt informationssäkerhetsarbete.
- Det ska finnas en nationell modell till stöd för ett systematiskt informationssäkerhetsarbete.

Att ha en god informationssäkerhet är viktigt för de flesta verksamheter för att nå upp till kvalitets- och effektivitetskraven. Att förbättra informationssäkerheten handlar därför inte enbart om att tillmötesgå externa krav, utan är även ett sätt att förbättra verksamheten. Samtidigt kan informationssäkerhet inte betraktas som enbart en verksamhetsintern angelägenhet. Flöden av tjänster och produkter sker i flera led, och bristande informationssäkerhet kan därför få följdverkningar långt utanför den egna verksamhetens gränser.

Ansvar, riskmedvetenhet och helhetssyn

Ett framgångsrikt informationssäkerhetsarbete förutsätter att det är tydligt vem eller vilka som har ansvar för det. Detta gäller på alla nivåer – både inom organisationer och i samhället i stort.

Såväl offentliga som privata aktörer behöver vara medvetna om att informationssäkerhetsrelaterade risker har en påverkan på målen för deras verksamhet samt att deras förmåga att hantera information även kan ha en påverkan på andra aktörer i samhället. Investeringar för att bygga in och förbättra säkerhet bör alltid jämföras med vad det kan kosta att inte göra detta. Målet är att hitta rätt säkerhetsnivåer och att de ansvariga är medvetna om vilka risker som finns, för att de aktivt ska kunna besluta om att eliminera, reducera eller acceptera dessa risker. En sådan riskmedvetenhet utgör grunden för effektiva investeringar i informationssäkerhet.

För att informationshantering och it-användning i samhället ska kunna utvecklas på ett tryggt och säkert sätt krävs att alla aktörer har en helhetssyn på informationssäkerhet. Informationssäkerhet är ett komplext och gränsöverskridande område som spänner över bl.a. teknik, administration, ekonomi och juridik. Informationssäkerhet ska vara en självklar och integrerad del i allt arbete på alla nivåer i samhället: inom och mellan organisationer samt inom och mellan samhällets olika

sektorer. Säkerhetsåtgärder bör både syfta till att skapa en mer robust informationshantering vid samhällets normaltillstånd och att hantera mer allvarliga störningar och kriser.

Nationell modell för systematiskt informationssäkerhetsarbete

I dagsläget bedriver de olika aktörerna i samhället sitt informationssäkerhetsarbete på delvis olika sätt, utifrån olika förutsättningar och behov, baserat på flera olika regelverk och delvis olika uppfattningar om hot och risker. Samma information kan få olika skydd i olika organisationer och kunskapen om vilket skydd som är lämpligt och tillgängligt för en viss typ av information är hos många aktörer ofullständig. När många aktörer är beroende av varandra i sin informationshantering är det också nödvändigt med samordnade åtgärder för att reducera risker och behålla säkerhetsnivån. Aktörer som har en sämre informationssäkerhet kan äventyra säkerheten för övriga. Detta har betydelse för möjligheterna till en digitalt samverkande förvaltning, men även för den återupptagna planeringen för civilt försvar som är beroende av goda förutsättningar att dela känslig information inom statsförvaltningen.

Även om den enskilda organisationen ytterst ansvarar för att hantera sin information är det enligt regeringens bedömning viktigt att förbättra förutsättningarna att bedriva ett systematiskt informationssäkerhetsarbete på ett mer samordnat sätt. För att åstadkomma detta behöver aktiviteter såsom att genomföra riskbedömningar, kartlägga skyddsvärda tillgångar och bestämma skyddsnivåer med tillhörande säkerhetsåtgärder genomföras med utgångspunkt i och stöd från en gemensam modell för systematiskt informationssäkerhetsarbete. En sådan modell syftar till att utgöra en gemensam plattform för det systematiska informationssäkerhetsarbetet och kan samordna och samla regelverk, metoder, verktyg, utbildningar med mera på myndighetsnivå på ett lättillgängligt sätt. En nationell modell bedöms bidra till att aktörer gör mer enhetliga bedömningar av hot, risker och säkerhetsåtgärder och att likartade uppgifter och informationssystem hos olika verksamhetsutövare därmed uppnår en likartad och adekvat skyddsnivå.

Det finns många fördelar med en nationell modell för systematiskt informationssäkerhetsarbete. Genom att de myndigheter som har ett särskilt ansvar på informationssäkerhetsområdet, och de övriga myndigheter som t.ex. har föreskriftsrätt eller tillsyn på området, aktivt bidrar i arbetet med den nationella modellen kan den motverka fragmentering av styrningen och öka samverkan inom området. Detta gör det enklare för organisationer att omhänderta relevanta krav och styra sitt informationssäkerhetsarbete samtidigt som expert- och tillsynsmyndigheternas kompetens används mer effektivt. Genom att den nationella modellen kommer att bygga på erkända standarder, vara flexibel och skalbar kan verksamheter med olika förutsättningar dra nytta av modellen.

Mer enhetliga bedömningar av säkerhetsåtgärder bedöms även kunna föra med sig positiva effekter för både dem som upphandlar säkerhetslösningar och dem som levererar dem. Att ta fram ett stort antal unika men snarlikna lösningar är inte rationellt vare sig för kund eller för

leverantör. En nationell modell skulle kunna bidra till att öka den samlade beställarkompetensen genom att den nationella modellen kan bidra med erfarenhetsbaserad kunskap om lämpliga krav.

Det främsta syftet med en nationell modell för systematiskt informationssäkerhetsarbete är att höja den lägsta nivån för informationssäkerhet. Modellen bör i första steget inriktas för statliga myndigheter, men bör utformas med målet att den ska kunna vara till nytta för hela den offentliga sektorn, andra organisationer och företag. Regeringens avsikt är att en nationell modell för systematiskt informationssäkerhetsarbete ska kunna utvecklas på ett sätt som även underlättar regeringens uppföljning av informationssäkerhetsarbetet i statsförvaltningen.

Regeringen ska verka för att

- öka tydligheten i myndighetsstyrningen och lyfta betydelsen av ett tillfredsställande informationssäkerhetsarbete internt på myndigheterna,
- förutsättningarna förbättras för samhällets olika aktörer att bedriva ett systematiskt informationssäkerhetsarbete och göra mer enhetliga bedömningar av hot, risker och säkerhetsåtgärder, genom att en nationell modell för systematiskt informationssäkerhetsarbete tas fram.

Samverkan och informationsdelning

Målsättning:
Samverkan och informationsdelning på informations- och cybersäkerhetsområdet ska stärkas.

Informationssäkerhetens komplexitet, gränsöverskridande karaktär och snabba utvecklingstakt kräver en effektiv samverkan. En god samverkan kring informationssäkerhet i samhället är viktigt under ett normaltillstånd, men också en nödvändighet för att man ska kunna skapa en god operativ förmåga att hantera allvarliga störningar. Den samverkan som byggs upp som en del av det förebyggande arbetet lägger ofta grunden för den samverkan som behövs vid allvarliga händelser. Det handlar om samverkan mellan olika aktörer i Sverige, som statliga myndigheter, kommuner och landsting, näringsliv och intresseorganisationer, men också om internationell samverkan (avsnitt 2.6).

Det finns flera goda exempel på samverkan på informationssäkerhetsområdet i Sverige. Samverkansgruppen för informationssäkerhet (SAMFI) spelar en viktig roll genom att verka för säkra informationstillgångar i samhället. SAMFI består av ett antal statliga myndigheter som har särskilda uppgifter på informationssäkerhetsområdet: Myndigheten för samhällsskydd och beredskap (MSB), Försvarets materielverk, Försvarets radioanstalt (FRA), Försvarsmakten, Polismyndigheten, Post- och Telestyrelsen (PTS) samt Säkerhetspolisen. MSB har det administrativa ansvaret för gruppen. Samverkansforumet Nationell samverkan till skydd mot

allvarliga it-hot (NSIT) analyserar och bedömer hot och sårbarheter när det gäller allvarliga eller kvalificerade it-angrepp mot våra mest skyddsvärda nationella intressen. NSIT består av Säkerhetspolisen, FRA och Försvarsmakten genom den militära underrättelse- och säkerhetstjänsten (MUST).

Regeringen ser ett behov av en utvecklad och fördjupad myndighetssamverkan för att höja informations- och cybersäkerheten i samhället. Ett exempel på detta behov är att ett antal nya myndigheter kommer att få nya uppgifter på informations- och cybersäkerhetsområdet när NIS-direktivet genomförs i svensk lagstiftning. Det är viktigt att samverkan utvecklas utifrån ett helhetsperspektiv.

Privat-offentlig samverkan är ett frivilligt, överenskommet samarbete mellan privata och offentliga aktörer. På informations- och cybersäkerhetsområdet finns flera exempel på plattformar för privat-offentlig samverkan. MSB har t.ex. etablerat ett antal forum för informationsdelning (FIDI) inom olika sektorer och områden: FIDI Telekom, Svenskt CERT-forum, FIDI Finans, FIDI Vård & Omsorg, FIDI Drift samt FIDI Supervisory Control And Data Acquisition (SCADA). Inom området för elektronisk kommunikation finns även Nationella telesamverkansgruppen (NTSG). NTSG är ett frivilligt samarbetsforum med syfte att stödja återställandet av den nationella infrastrukturen för elektroniska kommunikationer vid extraordinära händelser i samhället. Det finns ett behov av att fortsatt utveckla informationsdelningen gällande hot, risker och säkerhetsåtgärder i syfte att skyddet snabbt ska kunna anpassas hos fler aktörer.

Regeringen ska verka för att

- samverkan mellan myndigheter med särskilda uppgifter på informations- och cybersäkerhetsområdet stärks,
- ändamålsenlig informationsdelning och samverkan mellan privata och offentliga aktörer säkerställs.

Tillsyn på informationssäkerhetsområdet

Målsättning:
Det ska finnas en ändamålsenlig tillsyn som skapar förutsättningar för en ökad informations- och cybersäkerhet i samhället.

En förutsättning för att reglerna på informationssäkerhetsområdet ska få det genomslag som är avsett är att det finns en tillsyn som kan utföras på ett effektivt och ändamålsenligt sätt. Riksrevisionen har i sin rapport om informationssäkerhet i den civila statsförvaltningen (RIR 2014:23) pekat på behovet av tillsyn och rekommenderat ett antal åtgärder, bl.a. att utöka tillsynen av informationssäkerheten i den civila statsförvaltningen. Regeringen bedömer att ett flertal åtgärder behöver vidtas. I första hand behöver tillsynen av sådan verksamhet som omfattas av säkerhetsskyddslagstiftningen och samhällsviktig verksamhet inom de sektorer som pekas ut i NIS-direktivet utvecklas.

I säkerhetsskyddslagen finns bestämmelser om säkerhetsskydd. Med säkerhetsskydd avses skydd mot spioneri, sabotage och andra brott som kan hota rikets säkerhet, skydd i andra fall av uppgifter som omfattas av sekretess och som rör rikets säkerhet, och skydd mot terroristbrott, även om brotten inte hotar rikets säkerhet.

Enligt säkerhetsskyddslagstiftningen finns två huvudansvariga tillsynsmyndigheter, Säkerhetspolisen och Försvarsmakten, som i samråd med ansvariga myndigheter (Affärsverket svenska kraftnät, PTS, Transportstyrelsen och länsstyrelsen), även kan utöva tillsyn över sektorns myndigheter. Ansvariga myndigheter utövar också egen tillsyn över sektorn. Samtliga tillsynsmyndigheter har föreskriftsrätt.

I betänkandet En ny säkerhetsskyddslag (SOU 2015:25) anges bl.a. att samhällsutvecklingen medför att säkerhetskänslig verksamhet i högre grad än tidigare bedrivs av enskilda. En rimlig slutsats, enligt betänkandet, bör kunna vara att förekomsten av enskilda verksamhetsformer troligen kommer att öka inom tillsynsområdet men att det även i fortsättningen i huvudsak handlar om tillsyn av myndigheter och andra offentliga organ. Utredningen framhöll att tillgången till ingripandebefogenheter, t.ex. i form av sanktioner, är kännetecknande för en effektiv och ändamålsenlig tillsyn. I dag finns inte sådana befogenheter i fråga om säkerhetsskyddet. Utredningen gjorde ändå bedömningen att det då inte fanns tillräckliga skäl för att förändra tillsynens inriktning och genomförande. Något förslag om att införa sanktioner lämnades därför inte. Utredningen pekade dock på att det är angeläget att noga följa utvecklingen och inom en inte alltför avlägsen framtid följa upp frågan.

Regeringen har den 23 mars 2017 gett en särskild utredare i uppdrag att bl.a. utreda och föreslå ett system med sanktioner i säkerhetsskyddslagstiftningen (dir. 2017:32). Utredaren ska också genomföra en översyn av bestämmelserna om tillsyn enligt säkerhetsskyddslagen och lämna förslag om hur en ändamålsenlig tillsyn över säkerhetskänslig verksamhet ska vara utformad. Utredningen ska redovisas i maj 2018.

Genomförande av NIS-direktivet

NIS-direktivet fastställer åtgärder för att uppnå en hög gemensam nivå på säkerhet i nätverk och informationssystem inom unionen. Varje medlemsstat ska enligt direktivet utse en eller flera nationella behöriga myndigheter för säkerhet i nätverk och informationssystem för vissa tjänster i utpekade sektorer. De utpekade sektorerna är energi, transport, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, leverans och distribution av dricksvatten samt digital infrastruktur. De behöriga myndigheterna ska övervaka tillämpningen av NIS-direktivet på nationell nivå.

Regeringen gav i mars 2016 en särskild utredare i uppdrag att föreslå hur NIS-direktivet ska genomföras i svensk rätt (Ju 2016:11). Uppdraget redovisades nyligen genom betänkandet Informationssäkerhet för samhällsviktiga och digitala tjänster (SOU 2017:36). Utredaren har bl.a. föreslagit hur direktivets krav på utpekande av myndigheter med ansvar

för vissa funktioner ska genomföras, med inriktningen att MSB ges en samordnande roll på området men att andra myndigheter får ansvar för tillsyn inom de olika sektorerna. Utredaren har vidare föreslagit hur identifiering av och krav på aktörer som omfattas av direktivet kan genomföras i ett samlat regelverk med beaktande av gällande bestämmelser, sektorsansvar och vad som är mest effektivt utifrån olika perspektiv.

Regeringen ska verka för att

- säkerhetskyddslagstiftningen bättre möter de förändrade kraven på säkerhetsskydd inom informationssäkerhetsområdet, bl.a. genom ett adekvat system för sanktioner och en effektiv tillsyn,
- NIS-direktivet genomförs effektivt och att det etableras en adekvat styrning och tillsyn av säkerheten i nätverk och informationssystem i samhällsviktig verksamhet för vissa aktörer inom de utpekade sektorerna,
- behovet av ytterligare åtgärder för att utveckla tillsynen av informationssäkerheten i hela samhället bevakas.

2.2 Öka säkerheten i nätverk, produkter och system

Säker infrastruktur för elektronisk kommunikation

Målsättningar:
- Elektroniska kommunikationer ska vara effektiva, säkra och robusta samt tillgodose användarnas behov.
- Elektronisk kommunikation i Sverige ska vara tillgänglig oberoende av funktioner utanför landets gränser.
- Tillsynsmyndighetens behov av att kunna vidta adekvata åtgärder ska säkerställas.

Enskilda individer, statliga myndigheter, kommuner, landsting, företag och andra organisationer är i dag beroende av tillförlitliga elektroniska kommunikationstjänster som fungerar under alla förhållanden. Elektroniska kommunikationer med hög driftsäkerhet och starkt skydd är också av mycket stor vikt för samhällets funktionalitet och säkerhet samt möjligheter att hantera olika krisförlopp. Samhällsviktiga verksamheter som avser allmän ordning, säkerhet, hälsa och försvar har särskilt stora behov av säkerhet och robusthet.

Operatörer för elektronisk kommunikation är en heterogen grupp som i dag arbetar på en konkurrensutsatt marknad. En del äger sina egna nät medan andra hyr in sig i andra operatörers nät. Ägarförhållanden kan variera från stora börsnoterade aktiebolag via stadsnät till byalag. Det innebär i sig att aktörerna har olika förutsättningar för att förebygga och hantera incidenter och allvarliga händelser.

För att säkerställa konfidentialitet, riktighet och tillgänglighet i elektroniska kommunikationsnät och tjänster under såväl vardagsförhållanden som allvarliga kriser och höjd beredskap krävs ett kontinuerligt arbete med utgångspunkt i verksamhetsutövarnas risk- och

sårbarhetsanalyser och säkerhetsanalyser enligt säkerhetsskyddslagen. Alla operatörer bär också ett ansvar för att utveckla förmågan att förebygga, upptäcka och hantera incidenter.

Omvärldsförändringar påverkar kraven på säkerhet

Omfattningen av datahantering ökar i alla delar av samhället, med krav på ökad kapacitet, täckning, tillgänglighet och inte minst säkerhet i elektroniska kommunikationssystem. De gamla kopparnäten är under avveckling och ersätts med fiber och mobila kommunikationsnät. För att driva på den digitala utvecklingen och tillvarata dess möjligheter beslutade regeringen i december 2016 strategin Sverige helt uppkopplat 2025 – en bredbandsstrategi (N2016/08008/D), och i maj 2017 beslutades För ett hållbart digitaliserat Sverige – en digitaliseringsstrategi (N2017/03643/D). Inom EU pågår en översyn av regelverket för elektronisk kommunikation och OECD har initierat ett omfattande digitaliseringsprojekt. Policy och regelverk behöver förnyas oftare mot bakgrund av teknikutvecklingen och omvärldsförändringar.

Den säkerhetspolitiska utvecklingen har fått till följd att totalförsvarsplaneringen återupptagits. För att aktörer inom allmän ordning, säkerhet, hälsa och försvar ska kunna fullgöra sina uppdrag behöver de kunna kommunicera säkert med varandra, både i vardag och i kris. Ambitionen är att så långt som möjligt kunna upprätthålla elektroniska kommunikationer inom landet även i situationer där vårt närområde eller delar av landet har drabbats av olika typer av angrepp. Detta betyder att elektronisk kommunikation ska kunna fungera oberoende av funktioner i andra länder. Det betyder också att kraven på driftsäkerhet och robusthet ökar så att vi bättre ska kunna motstå angrepp och ytterst krig.

Stödet vid upphandling av säker elektronisk kommunikation och andra it-relaterade tjänster bör stärkas

Det är viktigt att de verksamheter som har behov av en hög nivå av driftssäkerhet på kommunikationsnät och it-relaterade tjänster ställer krav på detta vid upphandling. Det kan t.ex. handla om förmågan att snabbt och effektivt etablera alternativa förbindelser. Det är också viktigt att kunna identifiera och upphandla en för verksamheten lämplig nivå av driftsäkerhet. För detta krävs kompetens. PTS är tillsynsmyndighet inom postområdet och området för elektronisk kommunikation. Myndigheten verkar bl.a. för att aktörerna inom sektorn ska stärka sin förmåga att hantera allvarliga driftsstörningar, exempelvis genom att tillhandahålla stöd vid anskaffning av extern elektronisk kommunikation. MSB lämnar även stöd avseende säker upphandling av it-relaterade tjänster. Dessa stöd behöver nu utvecklas ytterligare. I sammanhanget kan också nämnas att Upphandlingsmyndigheten har det samlade ansvaret för att utveckla, förvalta och stödja den upphandling som genomförs av upphandlande myndigheter.

Behov av bättre beslutsunderlag och riktade åtgärder

En förutsättning för ett effektivt arbete med att förebygga hot och sårbarheter avseende elektronisk kommunikation är en utvecklad samordning och samverkan mellan berörda aktörer i syfte att identifiera

vad som ska skyddas och vilka ytterligare säkerhetsåtgärder som behöver sättas in. För att kunna analysera aktuella hot och sårbarheter behövs ett adekvat informationsunderlag. Detta underlag kan bestå av t.ex. information från operatörer inom elektronisk kommunikation genom incidentrapportering och information från expertmyndigheter. Flera tillhandahållare av elektronisk kommunikation kommer enligt NIS-direktivet att åläggas en utökad incidentrapportering. Incidentrapporteringen enligt NIS-direktivet beskrivs under avsnitt 2.3. Det kan emellertid behövas ytterligare åtgärder för att förbättra informationsunderlaget i syfte att stödja det förebyggande arbetet.

Som tillsynsmyndighet har PTS behov av att kunna inhämta, samordna och vidareförmedla information samt, under vissa omständigheter, vidta åtgärder för att stärka samhällets tillgång till säker elektronisk kommunikation. Vidare behöver PTS inhämta information från operatörerna om händelser med påverkan på nätsäkerhet eller informationssäkerhet för att kunna bedöma eventuella konsekvenser för samhället i stort. I detta ingår också att under en krissituation kunna skapa och vidareförmedla relevanta och aktuella lägesbilder. Det finns även ett behov för PTS att kunna rikta krav på specifika säkerhetsåtgärder mot en eller ett begränsat antal operatörer, för att hantera identifierade sårbarheter eller brister som kan medföra allvarliga risker för samhällsviktig elektronisk kommunikation. I dessa fall är sedvanliga föreskrifter inte lämpliga eftersom de gäller generellt på marknaden, inte enbart mot utpekade aktörer, och vanligen inte innehåller detaljerade krav på specifika nät och tjänster.

Behov av stärkt samverkan

För att kunna identifiera lämpliga åtgärder i syfte att minimera de hot och sårbarheter som finns inom sektorn för elektroniska kommunikationer behöver PTS tillgång till relevant kompetens. Denna kompetens kan hämtas från exempelvis sektorns aktörer och från expertmyndigheter. En fördjupad och systematisk samverkan såväl med sektorns aktörer som mellan myndigheter på informationssäkerhets- och tillsynsområdet utgör därför en god grund för ökat kompetensstöd till sektorsansvariga myndigheters informationssäkerhetsarbete.

Regeringen ska verka för att:

- elektroniska kommunikationsnät byggs på ett sådant sätt att de kan fungera oberoende av funktioner i andra länder,
- aktörer inom allmän ordning, säkerhet, hälsa och försvar har tillgång till moderna, säkra och robusta kommunikationslösningar,
- myndigheternas kompetens avseende upphandling av nätverk, produkter och system stärks och att myndigheterna vid upphandlingar säkerställer att hänsyn tas till säkerhetsaspekter,
- PTS förutsättningar att verka för en hög nivå av nät- och informationssäkerhet inom sektorn för elektronisk kommunikation stärks.

Målsättning:
Tillgången till säkra kryptosystem för it- och kommunikationslösningar ska motsvara behoven i samhället.

En vanligt förekommande säkerhetsåtgärd för att höja informationssäkerheten är användningen av krypto. Information som behöver skyddas med hjälp av krypto kan t.ex. utgöras av hälso- och sjukvårdsuppgifter, risk- och sårbarhetsanalyser, förundersökningar eller asylärenden, utöver information av vikt för rikets säkerhet.

Kryptolösningar används idag inte bara vid kommunikation i traditionell mening för att skydda information som omfattas av sekretess eller på annat sätt är skyddsvärd. Krypton används även till skydd för t.ex. signering av information (riktighet), automatiserade processer i samhällsviktiga funktioner som t.ex. kritiska infrastrukturer (tillgänglighet) och för att kunna följa hur och när information har hanterats och kommunicerats.

Vissa organisationer har behov av att skydda information som omfattas av sekretess med hänsyn till rikets säkerhet och behöver signalskydd. Begreppet signalskydd avser obligatoriskt skydd av elektronisk kommunikation av sekretessbelagda uppgifter som rör rikets säkerhet. Signalskyddssystemens skyddsnivå är dimensionerad att möta hotbilden från andra länders underrättelsetjänster och kräver därför omfattande skyddsåtgärder. Sverige behöver tillgång till teknisk kompetens inom kryptoområdet för att säkerställa nödvändigt signalskydd, såväl för den ordinarie verksamheten som vid tillfällen då samhället utsätts för påfrestningar. Att en sådan nationell kompetens bibehålls över tiden är därför viktigt för att trygga svenska säkerhetsintressen på området.

Behovet av säkra kryptolösningar ökar i takt med digitaliseringen. Även återtagandet av planeringen för det civila försvaret kommer att innebära ett ökat behov av säkra kryptosystem, framför allt signalskydd, för de aktörer i samhället som berörs av planläggningsarbetet. Det finns även ett ökat behov av signalskydd för att möjliggöra utvecklad samverkan med andra stater och internationella organisationer, inte minst inom EU och Nato.

För att möta det ökade behovet av kryptolösningar har regeringen sett ett behov av en nationell strategi och åtgärdsplan för säkra kryptosystem. Försvarets materielverk fick i regleringsbrevet för 2016 därför uppdraget att redovisa ett preciserat förslag till nationell strategi och åtgärdsplan för detta, efter samråd med Försvarsmakten, FRA och MSB.

Regeringen ska verka för att

– en nationell strategi och åtgärdsplan för säkra kryptosystem implementeras.

Målsättning:
Säkerheten i industriella informations- och styrsystem ska öka.

Industriella informations- och styrsystem, ofta benämnda Programmable Logic Controller (PLC) eller SCADA, används i samhällsviktiga verksamheter och kritisk infrastruktur för att styra och övervaka centrala fysiska processer. Styrsystemen (programvara och datorer) är integrerade i, och samverkar med, fysiska föremål. I och med framväxten av sakernas internet (Internet of things) ökar också antalet uppkopplade styrsystem kraftigt inom många områden.

Såväl betänkandet Informations- och cybersäkerhet i Sverige (SOU 2015:23) som betänkandet om en ny säkerhetskyddslag (SOU 2015:25) betonar samhällsviktiga verksamheters beroende av industriella informations- och styrsystem och vikten av att upprätthålla en stark nationell kompetens inom styrsystemområdet. Säkring av funktionaliteten och säkerheten hos industriella informations- och styrsystem utgör en mycket viktig del i såväl det förebyggande arbetet som i hanteringen vid störningar i centrala samhällsfunktionaliteter som el- och dricksvattensförsörjning. Även störningar inom områden som transportsystem, industriell produktion och sjukvård är exempel där förebyggande arbete är viktigt. Störningar kan ha sin grund i misstag vid handhavande eller bero på fel i maskin- eller programvara men kan även vara resultatet av antagonistiska aktiviteter.

Industriella informations- och styrsystem präglas av teknisk komplexitet samt mycket varierande ägar- och driftsförhållanden. För att hantera utmaningarna på området krävs ett samlat arbete som inkluderar både privat och offentlig sektor. Arbetet behöver bedrivas kostnadseffektivt och sektorsövergripande. För att uppnå ett adekvat skydd finns det ett behov av ökad samverkan och samarbete mellan systemleverantörer, tekniska konsulter, upphandlare, operatörer, relevanta myndigheter och akademiska miljöer.

En hög nivå av informations- och cybersäkerhet inom industriella informations- och styrsystem har möjlighet att utgöra en betydande konkurrensfaktor för Sverige. Om produkter med hög säkerhet kan utvecklas i Sverige kommer de att vara mer internationellt konkurrenskraftiga och därmed bidra till sysselsättningen i Sverige.

I dag bedrivs en stor del av utbildningen, forskningen och utvecklingen på området inom ramen för Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3), som drivs tillsammans av MSB och Totalförsvarets forskningsinstitut (FOI). Verksamheten vid NCS3 syftar till att minska de risker som användningen av industriella informations- och styrsystem medför för det moderna samhället, speciellt med avseende på avsiktlig störning. Även Myndigheten för Innovationssystem (Vinnova) och Research Instutes of Sweden (RISE), arbetar aktivt med projekt för utvecklad säkerhet i industriella informations- och styrsystem.

– företag och myndigheter som äger eller arbetar med samhällsviktig verksamhet där industriella informations- och styrsystem ingår får stöd i sitt arbete med att stärka informationssäkerheten,
– företag med verksamhet inom t.ex. verkstads- och processindustri där industriella informations- och styrsystem fyller viktiga funktioner får utvecklade förutsättningar till stöd för att stärka sitt arbete med informationssäkerhet.

2.3 Stärka förmågan att förebygga, upptäcka och hantera cyberattacker och andra it-incidenter

Målsättningar:
– Förmågan att förebygga, upptäcka och hantera cyberattacker och andra it-incidenter i samhället ska förbättras.
– Berörda aktörer ska kunna agera samordnat för att hantera cyberattacker och andra allvarliga it-incidenter.
– Det ska finnas ett utvecklat cyberförsvar för Sveriges mest skyddsvärda verksamheter med en förstärkt militär förmåga att möta och hantera angrepp från kvalificerade motståndare i cyberrymden.

Grunden för att minska effekterna av cyberattacker och andra it-incidenter består av förmågan att förebygga, upptäcka och hantera dessa.

En stor del av det förebyggande arbetet har beskrivits i kapitel 2.1 om att säkerställa en systematisk och samlad ansats i arbetet med informations- och cybersäkerhet och i kapitel 2.2 om ökad säkerhet i nätverk, produkter och system. Ytterligare en viktig komponent i det förebyggande arbetet utgörs av it-incidentrapportering som bl.a. möjliggör ett kontinuerligt lärande av inträffade händelser. De flesta statliga myndigheter är sedan april 2016 skyldiga att rapportera it-incidenter som allvarligt kan påverka säkerheten i myndighetens informationshantering till MSB. I syfte att förbättra den nationella lägesbilden ska MSB enligt sin instruktion årligen lämna en rapport till regeringen med en sammanställning av de incidenter som rapporterats in till myndigheten. Inför sammanställningen ska MSB inhämta upplysningar från Säkerhetspolisen och Försvarsmakten om de incidenter som rapporterats in till de myndigheterna i enlighet med säkerhetsskyddslagstiftningen. Nästa steg i att utveckla it-incidentrapporteringen kommer att tas genom NIS-direktivet. Det kommer bl.a. att innebära att det blir obligatoriskt för aktörer inom NIS-sektorerna att rapportera incidenter som har en betydande inverkan på kontinuiteten i samhällsviktiga tjänster. It-incidentrapporteringen kommer sammantaget att bidra till en förbättrad lägesbild i fråga om inträffade incidenter och effektiva säkerhetsåtgärder. Regeringen ser det som viktigt att metoder för att återkoppla information om inträffade it-incidenter till rapporterande aktörer utvecklas i syfte att stödja aktörernas förebyggande informationssäkerhetsarbete.

För att angrepp ska kunna upptäckas behöver det finnas tillgång till sensorer och andra mekanismer som detekterar händelser och sådan trafik som utgör en del av ett angrepp. FRA tillhandahåller ett tekniskt detekterings- och varningssystem (TDV) riktat till de mest skyddsvärda verksamheterna bland statliga myndigheter och statligt ägda bolag. Regeringen har under våren 2017 remitterat en promemoria om tekniska sensorsystem (Ju2017/02002/L4) med förslag att MSB får stödja verksamhetsutövare inom samhällsviktig verksamhet med informationssäkerheten genom att tillhandahålla sensorsystem som kan stärka samhällets möjlighet att upptäcka och hantera it-incidenter. MSB:s sensorsystem ska inte tillhandahållas till de verksamheter som erbjuds TDV. Särskilt utformade säkerhetsnät kan vara ytterligare en metod att värna skyddsvärd verksamhet från angrepp. Sådana nät kan vara gemensamma för flera myndigheter för att på ett kostnads- och resurseffektivt sätt upptäcka och försvåra angrepp.

För att hantera it-incidenter krävs en förmåga att motstå konsekvenserna av händelsen och att återställa system. Varje aktör som bedriver skyddsvärd eller samhällsviktig verksamhet har ett ansvar att utifrån relevanta riskanalyser, inklusive risk- och sårbarhetsanalyser och säkerhetsskyddsanalyser, utveckla beredskaps- och kontinuitetsplaner för att kunna hantera allvarliga cyberattacker eller andra it-incidenter. I samband med en it-incident kan en drabbad organisation vara i behov av externt stöd med hanteringen av incidenten. Sådant stöd kan erhållas av privata företag men även MSB erbjuder stöd genom CERT-SE som är Sveriges CSIRT-enhet (Computer Security Incident Response Team). Vissa statliga aktörer med särskilt skyddsvärd verksamhet har möjlighet att få stöd av FRA. Är det fråga om en it-incident som berör rikets säkerhet hanteras händelsen av Säkerhetspolisen och Försvarsmakten. I de fall händelsen har sin grund i brottsliga aktiviteter, genomför Polismyndigheten eller Säkerhetspolisen en brottsutredning.

Regeringens bedömning är att det finns ett behov att utveckla samhällets förmåga att på ett samordnat sätt agera för att motstå en cyberattack eller annan allvarlig it-incident. En sådan utvecklad förmåga är en viktig del i att stärka Sveriges totalförsvarsförmåga.

Cyberförsvar

Ett svenskt cyberförsvar som är tillräckligt robust för att stå emot och hantera cyberattacker, samtidigt som det är förberett för att vid behov snabbt kunna agera aktivt, kräver samordning och koordinering av kompetenser, samt utpekade och övade beslutsvägar, mellan olika myndigheter och samhällsfunktioner. Sveriges samlade cyberförsvarsförmåga utgår därför från en bred förståelse för att, och hur, de åtgärder som vidtas för att exempelvis höja lägstanivån i informations- och cybersäkerhetsarbetet hänger samman med arbetet att skydda samhället mot avsiktliga cyberattacker.

Grunden i en robust cyberförsvarsförmåga är att säkerställa funktionalitet i samhällsviktiga funktioner och skydda de mest skyddsvärda verksamheterna, inklusive sådana system som är vitala för totalförsvaret, mot antagonistiska angrepp från kvalificerade statliga eller statsstödda aktörer samt andra aktörer med liknande förmåga.

Regeringen bedömer att ett utvecklat cyberförsvar är ett kostnadseffektivt sätt att ytterligare höja tröskeln för en antagonistisk aktör som överväger att angripa Sverige eller svenska intressen eller utöva påtryckningar med militära eller andra maktmedel.

Ett effektivt nationellt cyberförsvar utvecklas och förstärks i fred och inom ramen för totalförsvarsplaneringen och ska kunna verka i fred, kris och krig. De verksamheter med informationssystem som måste kunna stå emot kvalificerade angrepp från stats- och statsstödda aktörer ska redan i fredstid utveckla ett skydd. Ett nationellt cyberförsvar förutsätter en stark nationell säkerhetstjänst och försvarsunderrättelseförmåga för att identifiera hotande verksamhet, både vad gäller aktörer och metoder, ett starkt skydd av de mest skyddsvärda verksamheterna i samhället, hög förmåga att detektera, varna för och hantera intrång och attacker, samt en robust förmåga att kunna genomföra aktiva operationer i cybermiljön.

Försvarsmakten ska upprätthålla och utveckla ett militärt försvar som ytterst kan möta ett väpnat angrepp. Cyberrymden är en av flera arenor där Försvarsmakten måste kunna agera. Försvarsmakten är den myndighet som ska verka inom alla delar av dator- och nätverksoperationer samt dimensionerat mot de högre konfliktnivåerna. Stöd från övriga berörda myndigheter är nödvändigt.

Internationell samverkan är viktig för att bl.a. utveckla den nationella cyberförsvarsförmågan och ska eftersträvas när så är lämpligt.

Regeringen ska verka för att

- det finns en samordnad planering mellan myndigheterna i händelse av en cyberattack eller annan allvarlig it-incident,
- verksamheter i behov av kontinuerlig bevakning och med särskilda behov av skydd får tillgång till ett sensor- eller detekterings- och varningssystem,
- ett effektivt och sömlöst cyberförsvar med förmågan att förebygga, upptäcka och hantera cyberangrepp, både för militär och civil verksamhet, fortsätter att utvecklas och förstärkas, vilket även inkluderar att Försvarsmakten utvecklar sin förmåga att försvara Sverige mot kvalificerade angripare i cyberrymden.

2.4 Öka möjligheterna att förebygga och bekämpa it-relaterad brottslighet

Målsättningar:
- De brottsbekämpande myndigheterna ska ha beredskap och förmåga att bekämpa it-relaterade brott på ett effektivt och ändamålsenligt sätt.
- Arbetet med att förebygga it-relaterade brott ska utvecklas.

Brå konstaterar att it-inslagen i de anmälda brotten ökar kraftigt (2016:17). Hit hör brott som begås med hjälp av internet som ett medel, t.ex. bedrägerier, och brott som innebär att det innehåll som förmedlas via internet är brottsligt, t.ex. barnpornografi eller hets mot folkgrupp. Ett

annat exempel är angrepp på it-system som sådana, t.ex. genom intrång eller överbelastningsattacker. En särskild kategori av it-relaterade brott är också de som innebär ett intrång i immateriella rättigheter. Även andra typer av brott såsom olaga hot och förtal förekommer via internet.

Till detta kommer att det i många förundersökningar finns relevant information eller bevisning att inhämta på internet eller i ett informationssystem, även om själva brottet inte har utförts i en sådan miljö.

Ett utmärkande drag för den it-relaterade brottsligheten är att den är gränsöverskridande, t.ex. genom överbelastningsattacker från ett land till ett annat eller bedrägerier som utförs från en server i ett land där det kan vara mycket svårt att utreda brotten. Det finns också många exempel på brott som inte har någon anknytning till andra länder än Sverige, men där information som är avgörande för utredningen finns hos ett företag i ett annat land. Detta kan gälla t.ex. hot och kränkningar på sociala medier.

Brå gör i sin rapport It-inslag i brottsligheten (2016:17) den sammanfattande bedömningen att rättsväsendet står inför stora framtida utmaningar och att de satsningar som hittills gjorts på it-området inte motsvarar behovet. Brå bedömer bl.a. att det finns ett stort behov av utbildning inom Polismyndigheten och Åklagarmyndigheten, att it-undersökarnas spetskompetens behöver säkerställas, att bemanningen inom den it-forensiska verksamheten behöver öka och att kunskapen vid myndigheternas expertfunktioner tillvaratas på ett bättre sätt.

Riksrevisionen drar i sin granskning av om Polismyndigheten och Åklagarmyndigheten har beredskap för att ändamålsenligt och effektivt handlägga och utreda it-relaterade brott slutsatser som delvis överensstämmer med Brås (RIR 2015:21).

Anpassning av lagstiftningen

I syfte att skapa bättre förutsättningar för att bekämpa it-relaterad brottslighet har regeringen vidtagit en rad åtgärder för att få en bättre anpassad lagstiftning. Flera ändringar har skett de senaste åren i den straffrättsliga lagstiftningen. Bl.a. har ett nytt brott, olovlig identitetsanvändning, införts i brottsbalken. Den 1 juli 2017 införs vidare i samma balk ett nytt brott, grovt fordringsbedrägeri, för att komma till rätta med problemen med bedrägerier med s.k. bluffakturor.

Det pågår även arbete med att ta fram förslag för att stärka det straffrättsliga skyddet för den personliga integriteten. Regeringen har i en lagrådsremiss den 8 juni 2017 föreslagit att skyddet mot hot och kränkningar stärks och moderniseras. Bland annat föreslås ett nytt brott som gör det straffbart att sprida vissa integritetskänsliga bilder och uppgifter. Vidare håller det på att tas fram förslag till förändringar i lagstiftningen som gäller kontakt med barn i sexuellt syfte, s.k. gromning, vilket många gånger sker via internet. Det har även initierats en översyn av barnpornografibrottet. Det pågår också ett arbete med att ratificera Europarådets konvention om it-relaterad brottslighet (ETS 185).

Vidare utreds för närvarande ett antal frågor som syftar till att modernisera lagstiftningen om tvångsmedel. Exempelvis utformades reglerna om beslag i brottsutredningar huvudsakligen före it-intåget i

samhället och är därför inte anpassade för tillämpning i it-miljöer. En annan fråga som utreds handlar om att beslut om hemlig avlyssning av elektronisk kommunikation blir allt svårare att verkställa eftersom de misstänkta i allt högre grad krypterar sin kommunikation.

För de brottsbekämpande myndigheterna är tillgång till uppgifter om elektronisk kommunikation mycket viktig för möjligheterna att utreda både it-relaterad brottslighet och annan brottslighet. EU-domstolen kom emellertid i ett förhandsavgörande den 21 december 2016 (i de förenade målen C-203/15 och C-698/15) till slutsaten att en generell och odifferentierad lagring av uppgifter om elektronisk kommunikation inte är förenlig med EU-rätten.

En särskild utredare ska därför föreslå de förändringar som är nödvändiga för att det svenska regelverket ska vara proportionerligt och ha en ändamålsenlig balans mellan skyddet för enskildas personliga integritet och behovet av uppgifter för att kunna förebygga, förhindra, upptäcka, utreda och lagföra brott.

Regeringen anser att det är angeläget att regelverket är effektivt och ändamålsenligt och att lagstiftningen är utformad så att nya typer av brottslighet kan motverkas.

Verksamhetsutveckling vid myndigheterna

För att bättre kunna förebygga, upptäcka, utreda och lagföra it-relaterade brott krävs inte bara en ändamålsenlig lagstiftning utan också att de brottsbekämpande myndigheterna utvecklar den organisation och kompetens som krävs. I regleringsbreven för 2017 gav regeringen Polismyndigheten och Åklagarmyndigheten i uppdrag att säkerställa en tillräcklig kompetens och beredskap när det gäller it-relaterad brottslighet. Bakgrunden till uppdraget var bl.a. Riksrevisionens och Brottsförebyggande rådets granskningar.

När det gäller sexualbrott mot barn har regeringen gett Polismyndigheten i uppdrag att dels identifiera områden där det finns ett utvecklingsbehov, dels genomföra lämpliga åtgärder. Uppdraget tar bl.a. sikte på internetrelaterade sexualbrott mot barn och dokumenterade sexuella övergrepp på barn. Uppdraget kommer att genomföras vid det nationella it-brottscentrum som inrättades inom Polismyndigheten den 1 oktober 2015: Swedish Cyber Crime Center (SC3). SC3 bildades i syfte att med stöd av sin expertkunskap säkerställa och utveckla utredningsstöd, arbetsmetoder, enhetlighet och internationellt samarbete när det gäller alla former av it-relaterad brottslighet.

Den snabba utvecklingen när det gäller it-relaterad brottslighet ställer stora krav på de brottsbekämpande myndigheternas förmåga att fortsatt utveckla sin verksamhet. Detta arbete bör enligt regeringen bedrivas kontinuerligt.

Brottsförebyggande arbete

När det gäller it-relaterad brottslighet är det, på samma sätt som med annan brottslighet, viktigt att i första hand minska inflödet till rättsväsendet och förebygga brott på ett tidigt stadium. Fler aktörer utöver de brottsbekämpande myndigheterna behöver aktivt delta i det förebyggande arbetet, inte minst spelar näringslivet en viktig roll. Andra

myndigheter än de brottsbekämpande och näringslivet kan t.ex. involveras i det förebyggande arbetet genom att bidra till att stärka samhällets kontrollfunktioner och utveckla tekniska lösningar för att öka säkerheten. I syfte att skapa bättre förutsättningar för ett strukturerat och långsiktigt brottsförebyggande arbete i hela samhället har regeringen bl.a. i mars 2017 överlämnat en skrivelse till riksdagen med ett nationellt brottsförebyggande program (Skr. 2016/17:126).

Internationellt samarbete mot it-relaterad brottslighet

Den tydliga gränsöverskridande dimensionen i den it-relaterade brottsligheten innebär att det internationella samarbetet har ökat i såväl omfattning som betydelse. Möjligheterna till samarbete genom EU och dess myndigheter Eurojust och Europol är de viktigaste för svenska brottsbekämpande myndigheter. Eurojust har bl.a. inrättat ett särskilt nätverk för åklagare som är specialiserade på it-relaterad brottslighet och vid Europol finns sedan några år ett it-brottscentrum. Båda dessa samarbetsmekanismer är viktiga för rättslig hjälp, t.ex. beslag och informationsutbyte.

På det politiska planet antog EU:s medlemsstater i juni 2016 rådsslutsatser om att förbättra det straffrättsliga samarbetet i cyberrymden. I slutsatsernas tre olika avsnitt behandlas utveckling av frivilligt samarbete med operatörer, effektivisering av det rättsliga samarbetet och frågan om exekutiv jurisdiktion (myndigheters rätt att på egen hand säkra bevisning) i cyberrymden i situationer där existerande regelverk inte är tillräckligt.

I september 2016 utvärderades vidare Sveriges förmåga att bekämpa it-relaterad brottslighet inom ramen för EU:s mekanism för ömsesidiga utvärderingar. En rapport med rekommendationer ska behandlas under våren 2017 och Sverige ska 18 månader efter rapportens antagande redovisa vidtagna åtgärder för att åtgärda identifierade brister.

Då många av de problem som svenska brottsbekämpande myndigheter står inför även återfinns i andra länder anser regeringen att det finns ett tydligt behov av att det internationella samarbetet på det här området, framför allt inom EU, fortsätter att utvecklas.

Regeringen ska verka för att

- lagstiftningen är anpassad för att effektivt kunna motverka den it-relaterade brottsligheten,
- de brottsbekämpande myndigheterna ges förutsättningar att, med hänsyn till skydd av den personliga integriteten och rättssäkerheten, upprätthålla sin förmåga att inhämta information,
- de brottsbekämpande myndigheterna säkerställer en adekvat organisation och tillräckliga resurser för att effektivt kunna förebygga och bekämpa den it-relaterade brottsligheten,
- de brottsbekämpande myndigheterna systematiskt arbetar för att utveckla kompetens och arbetsmetoder för att förebygga och bekämpa it-relaterad brottslighet,
- medvetenheten och kunskapen ökar hos andra aktörer än de brottsbekämpande om hur de kan bidra i arbetet med att förebygga it-relaterade brott,

– det internationella samarbetet mot it-relaterad brottslighet förstärks i syfte att bidra till en ökad lagföring i Sverige.

2.5 Öka kunskapen och främja kompetensutvecklingen

Kartläggning av sårbarheter och åtgärdsbehov

Målsättningar:
– Kunskapen i samhället som helhet om de mest angelägna sårbarheterna och behoven av säkerhetsåtgärder ska öka.
– Kunskapen hos enskilda användare av digital teknik om de mest angelägna sårbarheterna och behoven av säkerhetsåtgärder ska öka.

Det finns en stor utvecklingspotential avseende informations- och cybersäkerheten i Sverige, såväl på samhällsnivå som på individnivå. Kunskaper och resurser hos olika organisationer, och inte minst hos privatpersoner, om informations- och cybersäkerhet är dock ofta begränsade, varför det är viktigt att fokus kan riktas mot de mest angelägna behoven. Regeringen anser att det är centralt att de informationssäkerhetsåtgärder som vidtas är kostnadseffektiva.

MSB genomför i samarbete med berörda aktörer kartläggningar och undersökningar om informationssäkerhetsarbetet i samhället. MSB har bl.a., i nära samverkan med Sveriges kommuner och landsting (SKL), undersökt det systematiska informationssäkerhetsarbetet i kommunerna (MSB943). MSB:s analys av denna undersökning har utmynnat i åtta rekommendationer till kommunerna (MSB1045). Det är enligt regeringens bedömning viktigt att arbetet med att analysera sårbarheter, brister och behov med koppling till Sveriges informations- och cybersäkerhet fortsätter att utvecklas och fördjupas i syfte att stödja och öka medvetenheten om långsiktigt informationssäkerhetsarbete på alla nivåer i samhället.

På samma sätt som samhällets funktionalitet är beroende av it-system och it-tjänster är även den enskilde hänvisad till sådana system för att hantera allt fler delar i vardagslivet. Det handlar om betalningar, utbildning, kontakter med statliga myndigheter och kommuner med mera. I dag har nästan alla i Sverige tillgång till bredband med hög kapacitet både på arbetsplatsen och i hemmet.

Digitaliseringsstrategin (N2017/03643/D) lyfter fram att människor och organisationer ska känna tillit till och förtroende i användningen av digitala tjänster. Individen har alltid ett eget ansvar att skydda sin information och sina uppkopplade enheter, men det är även viktigt att samhället adresserar hot och risker som riktas specifikt mot enskilda vid deras användning av it-system och digitala tjänster. I dagsläget görs olika insatser för den enskildes informations- och cybersäkerhet av exempelvis Internetstiftelsen i Sverige, MSB, Polismyndigheten och andra aktörer. Dessa insatser är viktiga och behöver fortsatt utvecklas.

Regeringen ska verka för att

- berörda myndigheter utvecklar arbetet med att genomföra och stödja kartläggningar och utredningar om sårbarheter och lämpliga säkerhetsåtgärder i samhället,
- höja människors kunskap om sårbarheter och lämpliga säkerhetsåtgärder som var och en kan vidta för att skydda sig.

Högre utbildning, forskning och utveckling

Målsättning:
Det ska bedrivas högre utbildning, forskning och utveckling av hög kvalitet rörande informations- och cybersäkerhet och säkerhet på it- och telekomområdet i Sverige.

Utvecklingen inom it- och telekomområdet är ett naturligt steg i den alltmer globaliserade infrastruktur som byggs upp. Detta medför många möjligheter, men även att ökad forskning om digital säkerhet krävs för att kunna säkerställa att it-området förblir öppet, fritt och säkert.

I dag bedrivs forskning inom informations- och cybersäkerhetsområdet i varierande grad på flera svenska lärosäten. Tillämpad forskning inom informations- och cybersäkerhet sker bl.a. vid Totalförsvarets forskningsinstitut, Försvarshögskolan och Swedish Institute of Computer Sciences (RISE SICS).

Arbetet med att trygga samhällets informations- och cybersäkerhet behöver bedrivas på ett långsiktigt och effektivt sätt där grundläggande samhällsvärden, såsom skydd för personlig integritet, tillvaratas. Detta förutsätter att arbetet baseras på en såväl djup som bred kunskapsbas när det gäller behov, risker, sårbarheter, hot och möjligheter. Behovet av kompetent personal inom informationssäkerhetsområdet är också stort. Brist på spetskompetens drabbar såväl privat som offentlig sektor. Det bör därmed finnas ett gemensamt intresse hos samtliga berörda aktörer att hitta långsiktiga lösningar för att tillgodose de ökande behoven av kompetent arbetskraft.

Inom informations- och cybersäkerhetsområdet aktualiseras många komplexa forskningsfrågor som ofta kräver ett tvärdisciplinärt angreppssätt. Forskning inom t.ex. kryptoområdet är av avancerad teknisk karaktär medan forskning där individen står i centrum knyter an till t.ex. organisations- och beteendevetenskap. Utvecklingen av självstyrande bilar och intelligenta städer aktualiserar exempelvis både sociotekniska, juridiska och etiska frågor med direkt anknytning till informations- och cybersäkerhet.

I regeringens proposition Kunskap i samverkan – för samhällets utmaningar och stärkt konkurrenskraft (prop. 2016/17:50) presenteras ett antal strategiska forskningssatsningar inriktade mot särskilda områden varav ett är Forskningscentrum för framtidens teknik för digitalisering. Regeringen pekar i propositionen på att det är mycket viktigt att ny teknik som blir grunden i kritisk infrastruktur är robust och säker då adekvat säkerhet måste vara inbyggd i systemen från början. För att underlätta en sådan utveckling är det viktigt med en öppen tillgång till forskningsresultat. Regeringen anser att forskningsresultat, som

forskningsdata och vetenskapliga publikationer, som tas fram med offentlig finansiering ska vara öppet tillgängliga så långt det är möjligt.

Den 1 juni 2016 presenterade regeringen fem strategiska samverkansprogram som ska bidra till att möta flera av de samhällsutmaningar Sverige står inför. Det femte samverkansprogrammet, Uppkopplad industri och nya material, är inriktat på att stimulera en bred digitalisering av svensk industri genom en kraftsamling i form av samarbete mellan olika aktörer. Samverkan ska stärkas mellan etablerad industri, it- och telekomföretag, tjänsteföretag, innovativa unga företag i digitaliseringens framkant samt olika forskningsmiljöer, för att bättre bidra till att upprätthålla och öka den svenska konkurrenskraften. En särskild arbetsgrupp under samverkansprogrammet arbetar på att ta fram förslag till lösningar på informations- och cybersäkerhetsområdet. De strategiska samverkansprogrammen är ett viktigt instrument för att bidra till ökad kvalitet och nytta av högre utbildning, forskning och utveckling. En aspekt av detta är att olika aktörers investeringar vid behov kan samordnas och ge synergieffekter.

Det är regeringens bedömning att långsiktig samverkan och samarbete mellan berörda aktörer behöver fortsätta utvecklas på informations- och cybersäkerhetsområdet.

Regeringen ska verka för att

- lärosäten, industriforskningsinstitut, näringsliv och offentlig sektor samverkar för att öka nyttiggörande och innovation inom informations- och cybersäkerhetsområdet,
- informations- och cybersäkerhet beaktas i samtliga strategiska samverkansprogram.

Övningsverksamhet

Målsättning:
Det ska regelbundet genomföras både tvärsektoriella och tekniska informations- och cybersäkerhetsövningar i syfte att stärka Sveriges förmåga att hantera konsekvenserna av allvarliga it-incidenter.

En betydelsefull komponent för att öka kunskapen och stärka verksamheters förmåga att hantera allvarliga it-incidenter är utbildning och övning. Regelbundna nationella och internationella övningar är en förutsättning för att utveckla och utvärdera strukturer för hantering av allvarliga it-incidenter och för att identifiera organisatoriska, tekniska och administrativa utvecklingsbehov. Övningar kan användas för att

- validera policyer, planer, rutiner, utrustning och överenskommelser mellan organisationer,
- träna personal i fråga om deras roller och ansvar,
- förbättra samordning och kommunikation mellan organisationer,
- identifiera resursbrister, och
- identifiera förbättringsmöjligheter på både individ- och organisationsnivå.

Regeringen ser det därför som angeläget att berörda myndigheter och andra organisationer prioriterar att medverka i övningar inom informations- och cybersäkerhet. MSB upprätthåller förmågan att, i samverkan med andra berörda myndigheter, långsiktigt planera och samordna övningsverksamhet för att bygga kompetens och säkerställa en god förmåga att hantera allvarliga it-incidenter i samhället. Försvarsmakten upprätthåller motsvarande förmåga inom ramen för sitt ansvar.

Övningsverksamhet inom informations- och cybersäkerhetsområdet bör omfatta flera typer av övningar för att nå alla nivåer och kompetenser som behövs för att hantera allvarliga it-incidenter. Övningsverksamheten inkluderar alltifrån seminarieövningar till tvärsektoriella samverkansövningar. Tillgång till en virtuell övningsmiljö ökar väsentligt möjligheterna att genomföra tekniska cybersäkerhetsövningar. I en sådan miljö går det att öva på att hantera simulerade tekniska problem under förutsättningar som återspeglar verkligheten i form av tekniska infrastrukturer och system. På så vis kan deltagarna pröva sina processer och tekniska förmåga för att hantera incidenter och samtidigt utveckla samverkan med andra aktörer. Övningsverksamheten bör planeras på lång sikt så att varje enskild övning bidrar till att höja eller upprätthålla förmågan. Systematisk erfarenhetshantering blir en viktig del för att implementera resultat från övningarna i befintliga planer, arbetsmetoder och övrig verksamhet. Övningsverksamheten bör vidare vid behov ta hänsyn till andra hot och risker som kan ha en nära koppling till informations- och cybersäkerhetsområdet. Ett sådant exempel är informationspåverkan. Övningsscenarion inom informations- och cybersäkerhetsområdet som inkluderar informationspåverkan kan bidra till att höja samhällets samlade förmåga att motstå dessa hot inom såväl Försvarsmaktens försvarsplanering som totalförsvarsplanering. I dag genomförs en stor del av nationella och myndighetsspecifika tekniska övningar med stöd av FOI:s tekniska plattform CRATE (Cyber range and training enviroment).

Regeringen ska verka för att

– förmågan att hantera allvarliga it-incidenter upprätthålls genom en samordnad övningsverksamhet.

2.6 Stärka det internationella samarbetet

Utrikes- och säkerhetspolitik

Målsättning:
Internationella samarbeten kring cybersäkerhet ska stärkas, inom ramen för målsättningen om ett globalt, tillgängligt, öppet och robust internet som präglas av frihet och respekt för mänskliga rättigheter.

Digitalisering och globalisering har en accelererande betydelse för internationella relationer i stort. Det skapar nya möjligheter, men också nya konfliktytor, motsättningar och sårbarheter. Från att ha varit en avgränsad och teknisk angelägenhet, med fokus på system- och driftssäkerhet, har cybersäkerhet blivit en fråga med grundläggande relevans för fred, säkerhet och global utveckling. Staters agerande på cyberområdet får allt bredare och mer omfattande utrikes- och säkerhetspolitiska återverkningar.

Globalt finns motsättningar mellan stater kring hur cybersäkerhetsaspekterna ska hanteras. En huvudmotsättning rör synen på staters roll och rätt att övervaka, begränsa och kontrollera såväl infrastruktur som informationsflöden.

I dag behandlas frågor relaterade till informations- och cybersäkerhet från olika perspektiv i ett stort antal internationella organisationer och format, t.ex. FN, EU, OSSE, Europarådet, OECD och Nato, det nordisk-baltiska samarbetet, samt i flera specialiserade internationella organisationer och processer (t.ex. ICANN, IETF, ITU och IGF) som behandlar frågor som om drift, styrning och förvaltning av internet. Härutöver finns initiativ och processer med betydelse för den internationella diskussionen kring regler och normer, t.ex. den s.k. Londonprocessen, Freedom Online Coalition (FOC) och det svenska initiativet Stockholm Internet Forum (SIF).

Regeringen betonar vikten av att ytterligare utveckla Sveriges förmåga att agera samstämmigt och effektivt i internationella processer. Det kräver förbättrad överblick, där Sveriges långsiktiga intressen kan värnas inom ramen för ett stort antal processer som innefattar politiska, legala och tekniska aspekter. Det förutsätter också förbättrad samordning och dialog mellan berörda parter nationellt.

Frihet och säkerhet

Regeringens mål för internets utveckling är ett globalt, tillgängligt, öppet och robust internet som präglas av frihet och respekt för mänskliga rättigheter. För att frihetsdimensionen trovärdigt och effektivt ska kunna främjas krävs ett utvecklat internationellt samarbete för att hantera säkerhetsutmaningarna. Utvecklingen i omvärlden, inklusive i Sveriges närområde, understryker detta behov. Adekvata säkerhetsåtgärder kommer fortsatt behöva vidtas med hänsyn till nationell säkerhet eller för att bekämpa it-relaterad brottslighet.

Det finns samtidigt en risk att strävan efter kontroll över informationsflöden tar överhanden i många staters agerande. Tendenser till fragmentering och begränsning av internet går emot Sveriges grundläggande värderingar och långsiktiga ekonomiska och säkerhetspolitiska intressen. Regeringen framhåller att en sådan utveckling måste bemötas genom utvecklade internationella samarbeten.

Grundläggande motsättningar mellan stater finns också i synen på icke-statliga aktörers roller och ansvar. Regeringen vill motverka en statsledd förvaltning av internet och betonar de icke-statliga aktörernas centrala roller och ansvar för ett fritt och säkert internet, där legitima intressen hos näringsliv och civilsamhälle kan göra sig gällande. Det är tydligt att

såväl sårbarheter som säkerhetsåtgärder berör och involverar näringslivet och civilsamhället i stort. Samarbeten och dialog med icke-statliga aktörer behöver därmed fortsätta att utvecklas på internationell nivå.

Internationell rätt och internationella normer

Inom FN finns principiell samsyn kring att internationell rätt gäller på cyberområdet, men det finns betydande svårigheter och utmaningar att säkerställa att reglerna tolkas unisont. Mot denna bakgrund pågår internationella diskussioner kring tolkning och tillämpning av den internationella rätten på cyberområdet, liksom kring möjligheten att etablera frivilliga internationella normer och förtroendeskapande åtgärder för staters ansvarsfulla uppträdande. Här diskuteras även möjligheten att utifrån internationella regelverk, normer och överenskommelser verifiera, peka ut och utkräva ansvar. Regeringen betonar vikten av att Sverige tar en aktiv roll i dessa diskussioner och processer, med utgångspunkten att förebygga konflikter och understödja internationell samsyn kring normer för staters ansvarsfulla uppträdande.

Hot och sårbarheter

Angrepp och attacker inom cyberområdet utgör en växande utmaning. Stater kommer därför att vilja utveckla internationella samarbeten för att minska sin sårbarhet och stärka sin motståndskraft, bl.a. inom ramen för EU:s och Natos samarbeten för cybersäkerhet och cyberförsvar.

Cybersäkerhet måste också beaktas inom ramen för de framväxande hotbilder som kännetecknas av att en kombination av öppna och dolda instrument används antagonistiskt och destabiliserande, vilket också tydligt innefattar och berör det civila samhället i stort. Internationella samarbeten innefattar därmed också i allt större utsträckning den bredare frågan om påverkanskampanjer och desinformation, med potentiell inverkan på demokratiska processer, traditionella medier och sociala medier.

Regeringen verkar för utvecklade samarbeten inom EU, OSSE och med Nato, liksom i förhållande till utvalda strategiska samarbetsländer som delar Sveriges intressen. Samarbeten kring förutsättningarna i Sveriges närområde har särskild prioritet, t.ex. inom ramen för det svensk-finska, det nordiska och det nordisk-baltiska samarbetet.

Internationella standarder är en viktig fråga inom cybersäkerhetsområdet. Standarder utvecklas och förhandlas inom Europa och i andra internationella sammanhang och är en förutsättning för gränsöverskridande lösningar.

Mänskliga rättigheter och global utveckling

Mänskliga rättigheter gäller överallt. Regeringen framhåller att en rättighetsbaserad ansats bör vara en utgångspunkt i diskussioner som rör digitaliseringens möjligheter och utmaningar. Integritet och säkerhet på cyberområdet är en förutsättning för att individer ska kunna tillvarata och utöva sina fri- och rättigheter samt utnyttja informationsteknologins möjligheter.

Tillgång till ett öppet, fritt och säkert internet utgör ett viktigt instrument för att globalt stärka mänskliga rättigheter, demokrati,

rättsstatens principer och utveckling. Internet öppnar nya kanaler för människor att kommunicera, interagera och uttrycka sina åsikter och verka för sina intressen i en globaliserad värld i en omfattning som tidigare inte varit möjlig. Ökad tillgång till information och kunskap främjar också jämställdhet. Digitalisering och informationsteknologisk utveckling är i allt högre grad en betydande motor för ekonomisk och social utveckling, inte minst när det gäller att skapa förutsättningar för fattiga människor och kvinnors självständighet och möjlighet till arbete, samt för innovativa lösningar på utvecklingsproblem inom utbildning, finans, jordbruk, hälsa och miljö.

Regeringen ska verka för att

- stärka Sveriges samlade agerande som aktör inom relevanta internationella processer (inom bl.a. FN, EU, OSSE och i partnerskapet med Nato) och i samarbeten med likasinnade länder (i Norden, närområdet, inom EU och med globala partner),
- motverka tendenser till fragmentering av internet och begränsning av globala flöden,
- motverka en statsledd förvaltning av internet och värna de icke-statliga aktörernas roller och ansvar,
- stärka internationella samarbeten kring cybersäkerhet och cyberförsvar för att hantera hot och sårbarheter,
- stärka internationella samarbeten kring tillämpningen av internationell rätt och förebyggande av konflikter, t.ex. genom etablering av frivilliga normer och förtroendeskapande åtgärder,
- främja ett öppet, fritt och säkert internet till stöd för mänskliga rättigheter och global utveckling.

Handel och ekonomiskt samarbete

Målsättning:
Cybersäkerhet ska främjas inom ramen för ambitionen att värna fria flöden till stöd för innovation, konkurrenskraft och samhällsutveckling.

En fri handel som till fullo drar nytta av digitaliseringens möjligheter har stor potential att bidra till nya jobbmöjligheter, stärkt konkurrenskraft och hållbar tillväxt. De flesta företag, oavsett sektor, är i dag beroende av fria, gränsöverskridande dataflöden i sin verksamhet. Digitaliseringen innebär samtidigt ett stärkt intresse att värna upphovsrätt och säkerhet för företag i internationell konkurrens. Det är särskilt relevant för ett land som Sverige, med innovations- och kunskapsdrivna företag på en global marknad. En robust infrastruktur och en väl utvecklad cybersäkerhet är också väsentligt för att Sverige, i konkurrens med andra länder, ska kunna locka till sig investeringar. Regeringen framhåller vikten av att värna cybersäkerhet inom ramen för en övergripande ambition att främja innovation, konkurrenskraft och samhällsutveckling.

Fria dataflöden är en förutsättning för en välfungerande digital inre marknad och för handel med övriga världen. EU:s digitala inre marknadsstrategi syftar till att stärka och fördjupa den inre marknaden

med särskild relevans för politikområden som påverkas av digitaliseringen ur ett gränsöverskridande perspektiv. Fria dataflöden är också ett viktigt offensivt intresse för EU i de externa handelsförbindelserna mellan EU och omvärlden. Regeringen framhåller vikten av att fortsätta arbetet för att säkerställa att dataflöden inte hindras på den inre marknaden eller mellan EU och omvärlden. Hinder kan t.ex. bestå av omotiverade eller oproportionerliga lokaliseringskrav. Syftet med lokaliseringskrav är att tvinga företag att lokalisera data som annars hade förlagts i andra länder i det egna landet. Sådana hinder bör undanröjas samtidigt som vissa lokaliseringskrav med hänvisning till nationell säkerhet och andra offentliga intressen måste kunna anses motiverade.

Regeringen ska verka för att

- fortsätta Sveriges ledarskap inom EU på det digitala området och driva den digitala agendan framåt, genom att fullborda den digitala inre marknaden, liksom genom att vara drivande vad gäller diskussioner om framtidsfrågor,
- EU aktivt och offensivt motverkar digital protektionism samtidigt som legitima allmänna ändamål som dataskydd och nationell säkerhet respekteras.

3 Uppföljning av strategin

Regeringen vill med denna strategi skapa en tydlig plattform för Sveriges långsiktiga arbete med informations- och cybersäkerhet. Av strategin framgår vilka övergripande områden som regeringen vill prioritera och vilka målsättningar som finns för respektive område. Regeringen pekar även ut en övergripande inriktning för hur målsättningarna ska nås. Strategin kommer efter behov att följas av specifika uppdrag och andra styrande åtgärder till berörda myndigheter för att målsättningarna ska kunna nås.

Säkerhetsutmaningarna kommer inte kunna lösas en gång för alla. Teknik- och hotutvecklingen innebär att informations- och cybersäkerhetsområdet förändras och utvecklas i snabb takt. Detta återspeglas bl.a. i förändrade regler och krav på EU-nivå och internationellt. Strategin måste ha en flexibilitet att kunna anpassas till de snabba omvärldsförändringarna och är därför inte tidsatt, utan kommer att behöva uppdateras vid behov. Regeringens avsikt är att genomföra en första sådan uppdatering 2018 i syfte att anpassa strategin till de nya bestämmelser och övriga konsekvenser som genomförandet av NIS-direktivet i svensk rätt kommer att innebära.

Justitiedepartementet

Utdrag ur protokoll vid regeringssammanträde den 22 juni 2017

Närvarande: statsrådet M Johansson, ordförande, och statsråden Lövin, Hultqvist, Andersson, Hellmark Knutsson, Ygeman, A Johansson, Bolund, Damberg, Bah Kuhnke, Strandhäll, Fridolin, Eriksson, Linde, Skog, Ekström

Föredragande: statsrådet Ygeman

Regeringen beslutar skrivelse Nationell strategi för samhällets informations- och cybersäkerhet

Uppdatering om genomförandet av Nationell strategi för samhällets informations- och cybersäkerhet

Bilaga till Nationell strategi för samhällets informations- och cybersäkerhet, skr. 2016/17:213

Innehållsförteckning

1 Inledning 39

2 Styrningsram för genomförande av strategin 40
2.1 Syftet med styrningsramen 40
2.2 En översiktsbild av styrningsramen 41
2.3 Ansvar och roller i styrningsramen 41

3 En ny lag om informationssäkerhet för samhällsviktiga och digitala tjänster 44

4 Översikt över regeringens aktiviteter för att nå målen i strategin 45

1 Inledning

Ett år har gått sedan regeringen beslutade Nationell strategi för samhällets informations- och cybersäkerhet (skr. 2016/17:213). Ett tjugotal regeringsbeslut med koppling till strategin har beslutats under det gångna året. Det handlar bland annat om uppdrag till myndigheter med särskilda uppgifter på informations- och cybersäkerhetsområdet och som innebär åtgärder för en ökad informationssäkerhet hos såväl offentlig som privat sektor.

Regeringen har under de senaste åren arbetat för att stärka lagstiftningen på informations- och cybersäkerhetsområdet. En ny lag om informationssäkerhet för samhällsviktiga och digitala tjänster träder i kraft den 1 augusti 2018. Lagen genomför Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (NIS-direktivet) i svensk rätt. Den 1 april 2019 träder den nya säkerhetsskyddslagen i kraft.

Mycket arbete återstår för att nå samtliga målsättningar i strategin. Vi befinner oss bara i början av detta arbete. För att öka samverkan mellan samhällets olika aktörer, och därmed den samlade effektiviteten i genomförandet av strategin, har regeringen beslutat om en komplettering av strategin.

Syftet med kompletteringen är att utveckla och tydliggöra ansvar och roller för genomförandet av strategin i en styrningsram.

Kompletteringen innehåller vidare ett avsnitt om hur NIS-direktivet genomförts i svensk rätt.

Slutligen innehåller kompletteringen en översikt över regeringens pågående aktiviteter för att genomföra strategin.

2 Styrningsram för genomförande av strategin

2.1 Syftet med styrningsramen

Med styrningsram avses i detta fall ett ramverk som definierar roller och ansvar hos aktörer som är direkt inblandade i genomförandet av strategin. Styrningsramen tydliggör och utvecklar regeringens och myndigheternas arbete med att genomföra strategin, men förändrar inte några formella förhållanden dem emellan. Begreppet styrningsram kommer från artikel 7.1 b NIS-direktivet.

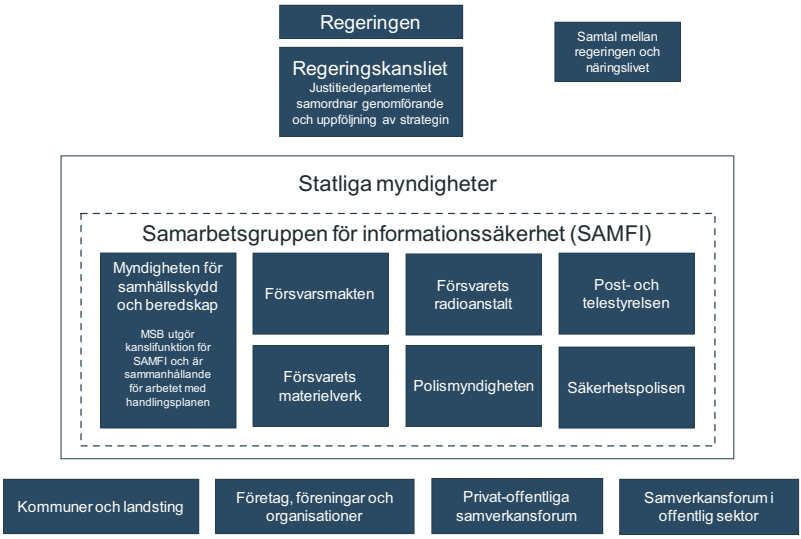
Informations- och cybersäkerhet är en fråga som angår hela samhället. Alla behöver ta sitt ansvar för informations- och cybersäkerhetsfrågor för att vi ska uppnå en effektiv och säker hantering av information. Statliga myndigheter, kommuner, landsting, företag och andra organisationer ska ha kännedom om hot och risker, ta ansvar för sin informationssäkerhet och bedriva ett systematiskt informationssäkerhetsarbete. Detta utgör en viktig målsättning i strategin.

Arbetet med informations- och cybersäkerheten inom varje enskild organisation ska ske i enlighet med ansvarsprincipen, gällande regelverk och bedrivas systematiskt och självständigt, men med stöd av de aktiviteter som genomförs inom ramen för styrningsramen.

Syftet med en tydlig styrningsram är först och främst att skapa fördjupad samverkan kring de aktiviteter som genomförs för att höja informations- och cybersäkerheten i samhället. Det vill säga aktiviteter som i många fall behöver genomföras i samverkan och påverkar fler aktörer än den egna organisationen.

Vissa aktiviteter kopplade till strategin inititeras av regeringen medan andra inititeras av myndigheter, enskilt eller i samverkan med t.ex. andra myndigheter, kommuner, landsting, företag eller andra organisationer. Styrningsramen ska bidra till en överblick över vilka aktörer som bidrar till genomförandet av strategin.

2.2 En översiktsbild av styrningsramen



- Regeringen har ansvaret för strategin.
- Justitie- och inrikesministern är det statsråd i regeringen som har ansvaret för att samordna genomförande och uppföljning av strategin.
- Samtal mellan regeringsföreträdare och näringsliv
- En tydligare roll för och ett särskilt uppdrag till myndigheterna i samarbetsgruppen för informationssäkerhet (SAMFI)
- Utvecklad samverkan och koordinering i förhållande till kommuner, landsting, företag och andra organisationer.

2.3 Ansvar och roller i styrningsramen

Regeringen och Regeringskansliet

Regeringen har ansvaret för strategin och fattar beslut om förändringar av de övergripande prioriteringarna för att stärka informations- och cybersäkerheten. Alla politikområden är i olika utsträckning berörda av informations- och cybersäkerhetsfrågorna. Justitie- och inrikesministern har ansvaret för att samordna genomförande och uppföljning av strategin. Övriga statsråd ansvarar för genomförande och uppföljning av strategin inom ramen för respektive departements ansvarsområden.

För att ta tillvara näringslivets kompetens och erfarenheter på informations- och cybersäkerhetsområdet kommer regeringsföreträdare även fortsatt ta initiativ till samtal med näringslivet.

Regeringskansliet har i uppdrag att stödja regeringen i dess uppgift att styra riket och förverkliga sin politik. Varje departement ansvarar för att löpande utveckla aktiviteter för att nå målsättningarna i strategin.

Justitiedepartementet samordnar genomförande och uppföljning av strategin i Regeringskansliet.

Regeringen avser att regelbundet begära in redovisningar av arbetet med informations- och cybersäkerhet hos de statliga myndigheterna. Vidare kan informationssäkerhetsområdets komplexitet och snabba utveckling leda till att regeringen vid behov kallar till sig myndigheter för särskilda avstämningar. Dessa redovisningar och avstämningar kommer utgöra en viktig del av regeringens samlade underlag och ligga till grund för beslut om uppdrag och andra styrande åtgärder till berörda myndigheter.

Statliga myndigheter

Det finns flera statliga myndigheter med särskilda uppgifter på informations- och cybersäkerhetsområdet, såväl nationellt som internationellt. Frågorna spänner över en mängd olika områden och nivåer. Strategin anger att samverkan mellan myndigheter med särskilda uppgifter på informations- och cybersäkerhetsområdet ska stärkas.

I samverkansgruppen för informationssäkerhet (SAMFI) finns en etablerad samverkan mellan Myndigheten för samhällsskydd och beredskap, Försvarsmakten, Försvarets radioanstalt, Post- och telestyrelsen, Polismyndigheten, Säkerhetspolisen och Försvarets materielverk.

Det finns också andra myndigheter som har uppgifter eller uppdrag som syftar till att höja informations- och cybersäkerheten för fler aktörer än den egna organisationen, t.ex. de myndigheter som kommer att utöva tillsyn med stöd av den kommande lagen om informationssäkerhet för samhällsviktiga och digitala tjänster samt Datainspektionen och Myndigheten för digital förvaltning, som inrättas den 1 september 2018. Andra exempel är Försäkringskassan, som har fått uppdrag relaterat till gemensam och säker it-drift hos ett antal myndigheter, Trafikverket, som tillhandahåller vissa it-system för förvaltning av och kapacitetstilldelning i järnvägssystemet till andra aktörer, samt Vetenskapsrådet, som finansierar forskning av betydelse för informations- och cybersäkerheten i samhället.

Alla statliga myndigheter under regeringen ska analysera om det finns sårbarheter eller risker inom myndighetens ansvarsområde som synnerligen allvarligt kan försämra myndighetens förmåga till verksamhet inom området. Myndigheterna ska minst vartannat år värdera och sammanställa resultatet av arbetet i en risk- och sårbarhetsanalys. Varje år lämnar Myndigheten för samhällsskydd och beredskap en nationell risk- och förmågebedömning till regeringen. Det är en analys som övergripande beskriver hot och risker och som bl.a. bygger på resultaten från myndigheternas risk- och sårbarhetsanalyser. Regeringen bedömer det som viktigt att risker, sårbarheter och åtgärder kopplade till informationssäkerhet fortsatt inkluderas och utvecklas i såväl arbetet med risk- och sårbarhetsanalyser som den nationella risk- och förmågebedömningen.

Uppdrag från regeringen för att höja samhällets informations- och cybersäkerhet kommer även fortsättningsvis riktas till såväl SAMFI-myndigheterna som andra myndigheter. Regeringen kommer att verka för en koordinering av alla uppdrag och uppgifter till statliga myndigheter.

Vad gäller internationellt arbete betonar regeringen i strategin vikten av att agera samstämmigt och effektivt vilket kräver förbättrad överblick över

ett stort antal internationella processer som innefattar politiska, legala och tekniska aspekter. Det förutsätter samverkan och informationsdelning såväl mellan berörda myndigheter som i förhållande till Regeringskansliet.

En tydligare roll för samverkansgruppen för informationssäkerhet

Försvarsberedningen konstaterade i sin rapport Motståndskraft, Inriktningen av totalförsvaret och utformningen av det civila försvaret 2021-2025 (Ds 2017:66), att det är centralt att bygga vidare på arbetet inom krisberedskapen och de strukturer för samhällets informations- och cybersäkerhet som redan är etablerade. Regeringen ser en fördjupad samverkan mellan myndigheterna i SAMFI som en viktig åtgärd för att stärka Sveriges informations- och cybersäkerhet. Tillsammans representerar dessa myndigheter en stor del av den spetskompetens svenska myndigheter har på informations- och cybersäkerhetsområdet. Flera av de utvecklingsbehov regeringen ser avseende samhällets informations- och cybersäkerhet kommer att kräva att dessa myndigheter löser uppgifter i nära samverkan.

Myndigheterna utgör även en kanal och mottagare för frågeställningar som rör olika typer av aktiviteter som övriga aktörer i samhället bedriver för att höja informations- och cybersäkerheten. Regeringen understryker vikten av informationsdelning mellan myndigheterna om deras samverkan med andra aktörer för att undvika överlappande arbete eller att centrala behov inte tillgodoses.

Regeringen har mot denna bakgrund gett myndigheterna i SAMFI ett uppdrag om en samlad informations- och cybersäkerhetshandlingsplan för åren 2019-2022. Handlingsplanen kommer att utgöra en samlad redovisning av vilka åtgärder SAMFI-myndigheterna på eget initiativ planerar att vidta för att höja informations- och cybersäkerheten i samhället inom ramen för sina befintliga ansvarsområden. De planerade åtgärderna ska utgå från målen i regeringens strategi.

För ett effektivt genomförande av strategin krävs att myndigheterna i så stor utsträckning som möjligt samordnar sitt arbete. Myndigheterna ska därför i sin egen planering och prioritering av verksamheten, när så är relevant för myndigheten, beakta arbetet med handlingsplanen för att ta tillvara effektivitets- och kvalitetsnyttor i arbetet med hela samhällets informations- och cybersäkerhet. Myndigheterna bör även på ett systematiskt sätt inhämta idéer och råd och i övrigt samverka med andra relevanta aktörer som kan bidra i arbetet. Företag är särskilt viktiga i det hänseendet liksom myndigheter, kommuner, landsting, Sveriges kommuner och landsting och andra organisationer. Det finns ett flertal etablerade samverkansforum på informations- och cybersäkerhetsområdet som vid behov kan nyttjas för detta ändamål.

I uppdraget ingår även att löpande hålla regeringen informerad om hur arbetet med handlingsplanen fortskrider.

Kommuner, landsting, företag och andra organisationer

Behovet av samverkan mellan den offentliga sektorn och näringslivet växer i betydelse. Den tekniska utvecklingen är i allt väsentligt styrd av

privata aktörer på marknaden. Privata aktörer äger och driver också stora delar av den samhällsviktiga verksamheten. Privata aktörer som hanterar affärshemligheter kan ha svårt att försvara sig mot angrepp som kan vara uthålliga, målinriktade och resursstarka. Sådana angrepp kan innebära hot mot svensk konkurrenskraft, och därmed sysselsättning och välstånd. Det innebär även att många privata aktörer behöver ett utvecklat stöd.

För kommunerna och landstingens del varierar nivån på informationssäkerheten. Det finns dock kommuner och landsting som har kommit längre i sitt informationssäkerhetsarbete och som har värdefulla kunskaper att bidra med. Sveriges Kommuner och Landsting (SKL) har arbetat med frågorna under en längre tid och byggt upp stöd för kommuners och landstings informationssäkerhetsarbete. SKL har också en viktig roll som kunskapsförmedlare mellan kommuner och landsting och statliga myndigheter.

Regeringen uppmuntrar och stödjer alla former av samarbeten mellan samhällets aktörer. När det finns ett engagemang för att hitta lösningar på gemensamma problem behöver det finnas tydliga ingångar till statliga myndigheter. I konkreta fall bör svar kunna ges på frågor om t.ex. vad det finns för stöd att tillgå från aktörer med särskild kompetens, om det pågår liknande arbeten med potentiella samordningsvinster eller om arbetet kan intressera fler samverkanspartners. Detta bidrar till en överblick över det arbete som pågår och vilka behov som finns på informations- och cybersäkerhetsområdet och säkerställer att pågående och planerade projekt kan nå sin fulla potential.

3 En ny lag om informationssäkerhet för samhällsviktiga och digitala tjänster

Nätverk och informationssystem spelar en allt viktigare roll i samhället. Deras tillförlitlighet och säkerhet är grundläggande för ekonomisk och samhällelig verksamhet och den inre marknadens funktion. Europaparlamentet och rådet antog därför 2016 ett direktiv om åtgärder för en hög gemensam nivå på säkerhet i nätverk och informationssystem inom hela EU, det s.k. NIS-direktivet.

I mars 2016 tillsatte regeringen en utredning med uppdrag att lämna förslag om hur NIS-direktivet ska genomföras i svensk rätt (dir. 2016:29). Den 29 mars 2018 beslutade regeringen en proposition där regeringen föreslår en ny lag om informationssäkerhet för samhällsviktiga och digitala tjänster (prop. 2017/18:205).

Den nya lagen träder i kraft den 1 augusti 2018 och kommer att kompletteras med en förordning om informationssäkerhet för samhällsviktiga och digitala tjänster.

4 Översikt över regeringens aktiviteter för att nå målen i strategin

Detta avsnitt innehåller information om vilka aktiviteter som regeringen arbetar med för att genomföra strategin. Avsnittet innehåller både genomförda och pågående aktiviteter. Aktiviteter som initieras av myndigheter eller som en följd av anslagsökningar till myndigheter för deras arbete med informationssäkerhetsfrågor ingår inte. Aktiviteter som är initierade av myndigheter kommer istället att redovisas i myndigheternas samlade handlingsplan.

Säkerställa en systematisk och samlad ansats i arbetet med informations- och cybersäkerhet

Uppdrag till bevakningsansvariga myndigheter att analysera och bedöma den egna informationssäkerheten. Redovisades den 1 mars 2018. (Ju2017/05787/SSK)

Regeringen beslutade om proposition Ett modernt och stärkt skydd för Sveriges säkerhet – ny säkerhetsskyddslag den 15 februari 2018 (prop. 2017/18:89). Lagen träder i kraft den 1 april 2019.

Uppdrag till MSB att i samverkan med Säkerhetspolisen och Försvarsmakten göra en samlad analys och bedömning av bevakningsansvariga myndigheters informationssäkerhetsanalyser. Redovisas den 1 oktober 2018. (Ju2017/05788/SSK)

Internt utvecklingsarbete för att utveckla myndighetsstyrningen i Regeringskansliet pågår.

Anpassning av lagstiftning till den allmänna dataskyddsförordningen pågår.

Uppdrag till MSB att verka för att de privat-offentliga samarbetsformerna stärks. Redovisades den 1 mars 2018. (Ju2017/05789/SSK)

Implementering av NIS-direktivet pågår. Regeringen beslutade om proposition Informationssäkerhet för samhällsviktiga och digitala tjänster den 29 mars 2018 (prop. 2017/18:205). Lagen träder i kraft den 1 augusti 2018.

Uppdrag till MSB att analysera och kartlägga informationssäkerheten inom landstingens hälso- och sjukvårdsverksamhet i samverkan med SKL och E-hälsomyndigheten pågår. Redovisas den 1 oktober 2018. (Ju2017/05789/SSK)

Särskilda uppdrag och återrapporteringskrav i regleringsbreven till flera myndigheter om deras interna informationssäkerhetsarbete pågår.

Uppdrag om en samlad informations- och cybersäkerhetshandlingsplan för åren 2019-2022. Handlingsplanen ska redovisas 1 mars 2019. Beslutades den 12 juli 2018.

Öka säkerheten i nätverk, produkter och system

Genom en förändring i säkerhetsskyddsförordningen har det införts krav på samråd med Säkerhetspolisen och Försvarsmakten inför utkontraktering av säkerhetskänslig verksamhet från den 1 april 2018.

Uppdrag till MSB och Trafikverket att redovisa ett specificerat underlag rörande utredningen Kommunikation för vår gemensamma säkerhet. Redovisades den 1 mars 2018. (Ju2017/09722/SSK)

Uppdrag till PTS att föreslå en förvaltningsmodell för skyddade it-utrymmen för offentliga aktörer som bedriver säkerhetskänslig verksamhet. Redovisades den 15 februari 2018. (Fi2017/03084/DF)

OECD översyn av digitalisering i Sverige ”Going digital: Policy Review of Sweden” publicerades den 15 juni 2018.

Försäkringskassan har fått i uppdrag att i år och under de kommande tre åren erbjuda samordnad och säker it-drift för vissa myndigheter. Redovisas den 18 december 2018. (Fi2017/03084/DF)

Uppdrag till Upphandlingsmyndigheten i 2018 års regleringsbrev att redovisa vilket stöd som ges vad gäller kravställning på informationssäkerhet vid offentlig upphandling.

Översyn inom EU av regelverket för elektronisk kommunikation pågår. KOM(2016) 590 slutlig.

Deluppdrag i utredningen *Radiospektrumanvändning i framtiden* kring nationella säkerhetsintressen vid tillståndsprövning. Redovisas den 31 december 2018. (dir. 2017:99)

Uppdrag till flera myndigheter avseende säkert elektroniskt informationsutbyte inom den offentliga sektorn. (Fi2018/02150/DF)

Uppdrag till flera myndigheter avseende säker och effektiv tillgång till grunddata. (Fi2018/02149/DF)

Frågan om ett utvecklat och säkert mobilt ip-baserat kommunikationssystem bereds i Regeringskansliet.

Stärka förmågan att förebygga, upptäcka och hantera cyberattacker

Uppdrag till FRA och Säkerhetspolisen om utveckling av arbetet till skydd för särskilt skyddsvärd verksamhet. Redovisades den 31 juli 2017. (Fö2017/00535/SUND)

Uppdrag till Försvarsmakten i 2018 års regleringsbrev att identifiera och redovisa åtgärder som kan bidra till att ytterligare utveckla arbetet för att skydda de mest skyddsvärda verksamheterna inom försvarssektorn i Sverige mot de allvarligaste hoten. Försvarsmakten ska inhämta synpunkter från Försvarets radioanstalt och Säkerhetspolisen som fick motsvarande uppdrag den 6 april 2017. Redovisas senast i samband med budgetunderlaget för 2019.

Rådsslutsatser om EU:s samordnade insatser vid storskaliga cyberincidenter och kriser antogs den 26 juni 2018. (10086/18 Cyber 139)

Uppdrag till FRA i 2018 års regleringsbrev att fortsätta att utveckla och placera ut tekniska detekterings- och varningssystem (TDV) vid skyddsvärda verksamheter. Redovisas den 1 oktober 2018.

Uppdrag till Försvarsmakten i 2018 års regleringsbrev att fortsätta analysera och utveckla förmåga att genomföra aktiva operationer i cybermiljön för ett förstärkt cyberförsvar. Uppdraget ska genomföras med stöd av FRA och eventuellt övriga berörda myndigheter. En redovisning av arbetsläget lämnades den 15 juni 2018.

Pågående EU-förhandling avseende EU:s cybersäkerhetsmyndighet (ENISA). (KOM(2017) 477 slutlig).

Öka möjligheterna att förebygga och bekämpa it-relaterad brottslighet

Regeringen beslutade den 22 juni 2017 propositionen Effektivare lagstiftning mot vuxnas kontakter med barn i sexuellt syfte (prop. 2016/17:214). Lagändringarna trädde i kraft den 1 januari 2018.

Regeringen beslutade den 31 augusti 2017 propositionen Ett starkt straffrättsligt skydd för den personliga integriteten (prop. 2016/17:222). Lagändringarna trädde i kraft den 1 januari 2018.

Uppdrag till Polismyndigheten och Åklagarmyndigheten i 2017 års regleringsbrev att återredovisa sina respektive åtgärder för att höja kunskapen avseende it-relaterad brottslighet. Redovisades i årsredovisningarna för 2017.

Uppdrag till Polismyndigheten och Åklagarmyndigheten att utveckla förmågan att bekämpa sexuella övergrepp mot barn. Uppdraget redovisades den 17 april 2018. (Ju2016/06827/PO)

Uppdrag till en utredare att överväga vissa frågor om barnpornografibrottet och om preskription ska avskaffas för sexualbrott och andra allvarliga brott mot barn. Redovisades senast den 18 juni 2018. (Ju 2017:H)

Beredning av betänkandet Datalagring – brottsbekämpning och integritet (SOU 2017:75) pågår.

Förhandling med anledning av EU-kommissionens förslag till ny förordning om myndigheters rätt att inhämta elektronisk bevisning direkt från leverantörer av elektroniska tjänster i andra medlemsstater samt ett direktiv med bestämmelser om utseende av juridisk representant i frågor som rör inhämtning av bevisning pågår.

Beredning av betänkandet Hemlig dataavläsning – ett viktigt verktyg i kampen mot allvarlig brottslighet (SOU 2017:89) pågår.

Beredning av betänkandet Beslag och husrannsakan – ett regelverk för dagens behov (SOU 2017:100) pågår.

Beredning av ratificering av Europarådets konvention om it-relaterad brottslighet (ETS 185) pågår.

Öka kunskapen och främja kompetensutvecklingen

Uppdrag till MSB att stärka allmänhetens samt små och medelstora företags motståndskraft mot it-incidenter och kunskap om informationssäkerhet. Redovisas den 31 januari 2019. I uppdraget ingår att genomföra en nationell informationskampanj. (Ju2018/01866/SSK)

Pågående EU-samarbete om etablerande av ett nätverk av cybersäkerhetscentra och ett Europeiskt forsknings- och kompetenscentrum för cybersäkerhet. (Arbetet utgår från handlingsplan 15748/17 som antogs den 12 december 2017.)

Uppdrag till MSB i 2018 års regleringsbrev att utveckla sitt arbete med att stödja och samordna samhällets informationssäkerhet.

Uppdrag till MSB att uppdatera och vidareutveckla metodstödet till kommunerna samt genomföra riktade utbildningsinsatser mot kommuner, landsting och länsstyrelser. Redovisas den 1 april 2019. (Ju2018/02265/SSK)

Pågående EU-förhandling om att utveckla ett europeiskt ekosystem med superdatorer (EuroHPC).

Stärka det internationella samarbetet

Avslutade förhandlingar av cybersäkerhetspaketet hösten 2017. (JOIN(2017)450 final)

Pågående arbete i rådsarbetsgrupper och kommittéer inom EU t.ex. HWP Cyber, COSI och ERAC.

Pågående arbete inom Europol mot it-relaterad brottslighet.

Pågående medverkan i relevanta FN-processer med relevans för cybersäkerhet, i första hand generalförsamlingens första utskott, rådet för mänskliga rättigheter och IGF (Internet Governance Forum)

Pågående medverkan i internationella konferenser och dialoger kring stabilitet och säkerhet i cyberrymden (t.ex. Global Commission on the Stability of Cyberspace)

Antagande hösten 2017 av ramverk för EU:s diplomatiska verktygslåda för bemötande av cyberattacker (Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities). Medverkan igenomförande av verktygslådan.

Pågående arbete inom det nordiska samarbetet i frågor om informations- och cybersäkerhet.

Pågående arbete i OSSE om bland annat förtroende-skapande åtgärder för hantering av cyberincidenter med säkerhetspolitiska återverkningar.

Bilaterala dialoger inom Norden, EU och globalt.

Pågående arbete i Freedom Online Coalition för främjandet av ett fritt och öppet internet.

Justitiedepartementet
Regeringskansliet
103 33 Stockholm

08-405 10 00
regeringen.se/justitie