STATSRÅDETS PRINCIPBESLUT OM EN FÖRBÄTTRING AV INFORMATIONSSÄKERHETEN OCH DATASKYDDET INOM KRITISKA SAMHÄLLSSEKTORER

INNEHÅLL

1 Inledning

Samhällets olika sektorer blir alltmer beroende av digitala tjänster, både i Finland och på global nivå. Viktiga tjänster i samhället, såsom distributionen av el och dricksvatten samt hälso- och sjukvårdstjänsterna, behöver tillförlitliga förbindelser och datasystem för att fungera. I de olika sektorerna är det viktigt att aktivt agera för att förbättra informationssäkerheten och data-skyddet och identifiera betydelsen av säkerhetenshelhet för tjänsternas kvalitet och säkerhet i det digitala samhället.

Lagstiftningen, framför allt personuppgiftslagar och allmänna lagar som gäller myndigheter, innehåller allmänna skyldigheter i fråga om informationssäkerhet och dataskydd. I Finland finns det dessutom för många sektorer specifika skyldigheter att sörja för informationssäkerheten och dataskyddet för tjänster och informationssystem. Bra exempel på sådana sektorer med specifika skyldigheter är kommunikations- och finanssektorerna. Det finns emellertid stora skillnader mellan de olika sektorernas kapacitet att möta de växande utmaningarna i fråga om informationssäkerhet och dataskydd. För de olika samhällssektorerna fastställs från varandra avvikande krav på informationssäkerhet och dataskydd där man strävar efter att beakta respektive sektors särdrag. En samordning av lagstiftningen med kraven i EU:s dataskyddsbestämmelser pågår fortfarande, även om flera ministerier redan har genomfört reformer. Enbart lagstadgade skyldigheter och föreskrifter räcker dock inte för att förbättra informationssäkerheten och dataskyddet, utan skyldigheterna kompletteras av verksamhetskulturen inom de olika sektorerna, en gemensam lägesbild, förståelse för förändringarna i omvärlden och ett frivilligt samarbete mellan myndigheter och tjänsteleverantörer.

Störningar och kränkningar av informationssäkerheten och kränkningar av dataskyddet kan i hög grad påverka verksamheten och tjänsterna inom olika sektorer. Detta gäller numera även föremål, anordningar och fordon, som i allt större omfattning är kopplade till internet och som styrs genom behandling av digital information. Nivån på informationssäkerheten för de förbindelser, tjänster och anordningar som används påverkar direkt medborgarnas förtroende för digitala tjänster och produkter. Produkter, tjänster och informationssystem måste planeras, tillverkas och underhållas på ett sådant sätt att informationssäkerheten och dataskyddet utgör en oskiljaktig och integrerad del av dem. Med andra ord måste informationssäkerheten och dataskyddet under hela livscykeln utgöra utgångspunkt för utvecklingen av produkter, system och tjänster.

Ökade kunskaper om och förståelse för den digitala verksamhetsmiljön samt instruktioner till privata och offentliga organisationer och enskilda användare om fungerande och säkra verksamhetsmodeller spelar en viktig roll i det digitala samhället och när det gäller att öka medborgarnas förtroende. Det är i hög grad även en fråga om riskhantering, och de olika aktörerna måste gripa sig an denna fråga för att deras nätverk och informationssystem ska förbli säkra och kunna stå emot störningar. För företag kan störningar och kränkningar orsaka omfattande ekonomiska skador, och i ett större perspektiv kan störningar påverka försörjningsberedskapen och tillgången till grundläggande tjänster i hela samhället.

Det dataintrång som psykoterapicentret Vastaamo utsattes för visade hur ett dataintrång eller en cyberttack i hög grad påverkar vanliga människors vardag och avslöjar mycket känsliga uppgifter om deras liv. Dataintrång och kränkningar av dataskyddet kan utöver att de får ekonomiska konsekvenser även orsaka stort mänskligt lidande, vars betydelse som ett samhälleligt och rättsligt missförhållande inte ska underskattas. Den offentliga maktens uppgift är att med stöd av grundlagen trygga skyddet för medborgarnas privatliv och andra grundläggande fri- och rättigheter. En tillräcklig säkerhetsnivå kan dock inte uppnås enbart genom myndighetsåtgärder, utan hela samhället måste bli medvetet om informationssäkerhetens och dataskyddets betydelse och även aktörer inom den privata sektorn måste förbinda sig till detta.

Utredningen av de olika aspekterna av det dataintrång som Vastaamo utsattes för visade att det i Finland finns informationssystem där nivån på informationssäkerheten, dataskyddet och övervakningen inte är tillräcklig enligt EU:s dataskyddslagstiftning och speciallagstiftningen för den aktuella sektorn. En del av dessa system finns inom sektorer som är kritiska för samhällets verksamhet. Övervakningen av dessa system har inte heller varit up-to-date och därför kan utgångspunkten anses vara att regleringen och tillsynen av sådana informationssystem måste förstärkas. En resultatrik utveckling av verksamheten förutsätter utöver reglering, instruktioner och tillsyn att de ekonomiska resurserna riktas på ett effektivt sätt både inom den offentliga sektorn och i näringslivet. I sista hand ansvarar dock företagen och myndigheterna själva för nivån på informationssäkerheten och dataskyddet för de egna tjänsterna, produkterna och informationssystemen. Staten har som uppgift att ansvara för en tillräcklig övervakning av informationssäkerheten.

För dataskyddets del är det viktigt att notera att informationssäkerhet endast är en metod att skydda personuppgifter. Andra metoder är till exempel att minimera mängden personuppgifter som behandlas så att de endast omfattar nödvändiga uppgifter och att behandla uppgifter på ett sådant sätt att de inte direkt kan kopplas till en enskild person. I detta principbeslut behandlas dataskyddet huvudsakligen ur ett informationssäkerhetsperspektiv. Detta minskar dock inte betydelsen av andra principer och bestämmelser som styr behandlingen av personuppgifter när det gäller att trygga dataskyddet och den informerade självbestämmanderätten för medborgarna. När det gäller de termer som används i principbeslutet bör det noteras att cybersäkerhet och informationssäkerhet används synonymt i beslutet.

Riktlinjerna i principbeslutet grundar sig på en utredning som gjordes av en tväradministrativ arbetsgrupp under ledning av kommunikationsministeriet och som publicerades den 1 februari 2021[1]. I Finland har utvecklingen av cybersäkerheten behandlats ingående i den strategi för cybersäkerheten i Finland som färdigställdes 2019 och i det genomförandeprogram för strategin som färdigställs våren 2021[2]. Vid genomförandet av strategin för cybersäkerheten fokuserar man särskilt på långsiktiga åtgärder för att utveckla cybersäkerheten, såsom en förbättring av kunskaps- och informationssäkerhetskulturen. Därför behandlas motsvarande långsiktiga åtgärder, som exempelvis gäller internationellt samarbete, kunskaper eller övningsverksamhet, inte i detta principbeslut. Avsikten är att genomförandeprogrammet och åtgärderna i detta principbeslut ska utgöra en enhetlig helhet och stödja varandra, så att de utmaningar som informationssäkerheten och dataskyddet innebär kan mötas på både kort och lång sikt. Målet är ett samhälle med världens mest tillförlitliga och säkra digitala tjänster för alla samhällsaktörer.

2 Politiska riktlinjer

2.1 Myndigheterna bör samarbeta samt bistås och förstärkas av Cybersäkerhetscentret

1. En gemensam författningsgrund bör skapas för myndighetssamarbete i situationer där informationssäkerheten har kränkts. En lag om samarbete mellan myndigheter i syfte att förhindra och utreda kränkningar av informationssäkerheten bör innehålla bestämmelser om tillsättandet av en samarbetsgrupp i situationer där informationssäkerheten har kränkts, om föregripande och

[1]Förbättring av informationssäkerheten och dataskyddet inom kritiska sektorer i samhället: Arbetsgruppens slutrapport (Kommunikationsministeriets publikationer 1/2021), http://urn.fi/URN:ISBN:978-952-243-614-6).

[2] https://turvallisuuskomitea.fi/sv/strategi-for-cybersakerheten-i-finland-2019/.

händelsespecifikt informationsutbyte mellan myndigheter samt om tillfälligt överlåtande av utrustning, lokaler och personal till en annan myndighet. Vid beredningen av författningsgrunden bör man även bedöma om nuvarande samarbetsförfaranden som har konstaterats fungera bra bör förstärkas samt samarbetet med den privata sektorn. Det bör säkerställas att myndigheterna har tillräckliga resurser för ett samarbete.

Ansvarig aktör: KM, samarbetsmyndigheternas övriga förvaltningsområden

Resurskonsekvenser: Lagberedning som tjänsteuppdrag inom ramen för de nuvarande resurserna, den nya regleringen kan medföra ytterligare resursbehov för myndigheterna.

Tidsplan för åtgärden: Angelägenhetsgrad 1 (bör genomföras inom 1–2 år)

2. Tillräckliga resurser för myndighetstillsyn bör säkerställas ur statsbudgeten för att riktlinjerna i denna rapport ska kunna genomföras.

Ansvarig aktör: KM, FM, SHM, ANM, JM, JSM, IM

Resurskonsekvenser: Kräver ytterligare finansiering.

Tidsplan för åtgärden: Angelägenhetsgrad 1 (bör genomföras inom 1–2 år från det att man avtalat om finansieringen)

3. Kommunikationsministeriets resurser bör utökas så att de motsvarar den ökande arbetsmängd som cybersäkerheten medför och cybersäkerhetens betydelse i samhället.

Ansvarig aktör: KM

Resurskonsekvenser: Kräver ytterligare finansiering.

Tidsplan för åtgärden: Angelägenhetsgrad 1 (bör genomföras inom 1–2 år från det att man avtalat om finansieringen)

4. Cybersäkerhetscentret vid Transport- och kommunikationsverket bör få utökade resurser så att det kan stödja andra förvaltningsområden och erbjuda dem sektorsspecifik rådgivning. Vid Cybersäkerhetcentret bör det inrättas en separat sakkunnigtjänst för varje kritisk sektor, där de ansvariga tjänstemännen på heltid stöder den sektorsmyndighet som ansvarar för informationssäkerheten inom en viss sektor.

Ansvarig aktör: KM, Transport- och kommunikationsverket, NIS-sektorsmyndigheterna

Resurskonsekvenser: Kräver ytterligare finansiering.

Tidsplan för åtgärden: Angelägenhetsgrad 1 (bör genomföras inom 1–2 år från det att man avtalat om finansieringen)

5. Cybersäkerhetscentret vid Transport- och kommunikationsverket bör erbjuda utbildning för de myndigheter som utför tillsyn av informationssäkerheten i NIS-sektorerna. Arbetsgivarämbetsverken bör förbinda sig att göra Cybersäkerhetscentrets utbildning eller annan motsvarande utbildning i informationssäkerhet obligatorisk för tjänstemän som arbetar med tillsyn av informationssäkerheten. Arbetsgivarämbetsverken bör, baserat på utbildningen, kunna visa att de sakkunniga som arbetar med tillsyn av informationssäkerheten har tillräckliga kunskaper.

Ansvarig aktör: Transport- och kommunikationsverket, NIS-sektorsmyndigheterna

Resurskonsekvenser: Kräver ytterligare finansiering.

Tidsplan för åtgärden: Angelägenhetsgrad 2 (bör genomföras inom 2–4 år från det att man avtalat om finansieringen)

6. Den tjänst för kartläggning av informationssäkerheten som erbjuds av Cybersäkerhetscentret vid Transport- och kommunikationsverket bör göras tillgänglig för alla kritiska sektorer. Med hjälp av tjänsten är det möjligt att upptäcka och åtgärda sårbarheter i icke-lokala nätverks informationssäkerhet. Nödvändiga ändringar i lagstiftningen bör göras. Det bör säkerställas att myndigheterna inom de kritiska sektorerna har tillräckliga kunskaper för att kunna tolka resultaten av kartläggningstjänsten.

Ansvarig aktör: KM, Transport- och kommunikationsverket

Resurskonsekvenser: Kräver ytterligare finansiering.

Tidsplan för åtgärden: Angelägenhetsgrad 2 (bör genomföras inom 2–4 år från det att man avtalat om finansieringen)

7. Myndigheternas behov av tekniska lösningar för att skapa miljöer för behandling av sekretessbelagda och säkerhetsskyddsklassificerade uppgifter bör utredas. Utredningen bör bland annat omfatta enhetlig och krypterad e-post mellan myndigheter, säkra mötesförbindelser och mötestjänster samt en säker dataöverföringstjänst. Utredningen bör göras 2021, varefter moderna lösningar bör utformas och genomföras 2022–2023 med utgångspunkt i utredningen. Utredningen bör även omfatta en utvärdering av kompatibiliteten när det gäller informationsutbytet mellan myndigheter och utomstående aktörer.

Ansvarig aktör: FM

Resurskonsekvenser: Kräver ytterligare finansiering.

Tidsplan för åtgärden: Angelägenhetsgrad 1 (bör genomföras inom 1–2 år från det att man avtalat om finansieringen)

8. Det bör säkerställas att systemet Havaro, som används för att upptäcka och varna för kränkningar av informationssäkerheten, i stor utsträckning är tillgängligt för de kritiska sektorerna. Nödvändiga lagstiftningsändringar bör göras så att tjänsten Havaro kan erbjudas fler aktörer än för närvarande.

Ansvarig aktör: KM, Transport- och kommunikationsverket

Resurskonsekvenser: De nuvarande resurserna är tillräckliga.

Tidsplan för åtgärden: Angelägenhetsgrad 2 (bör genomföras inom 2–4 år)

2.2 Lagstadgade informationssäkerhetskrav bör införas för alla kritiska sektorer

9. Tydliga och proportionerliga informationssäkerhetskrav för kritiska sektorer bör fastställas i lagstiftningen. Kriterierna bör fastställas med utgångspunkt i riskerna. Myndigheterna måste genom lag ges tillräckliga befogenheter att meddela bindande föreskrifter om informationssäkerhet för kritiska sektorer. Befintliga föreskrifter bör ses över för att säkerställa att de är aktuella. Vid utarbetandet av informationssäkerhetskrav bör internationell lagstiftning och de begränsningar och krav som fastställs i den beaktas.

Ansvarig aktör: KM, ANM, JSM, SHM, FM

Resurskonsekvenser: Lagberedning som tjänsteuppdrag inom ramen för de nuvarande resurserna med undantag av FM där behovet är 0,5 årsverken, den nya regleringen kan medföra ytterligare resursbehov för myndigheterna.

Tidsplan för åtgärden: Angelägenhetsgrad 2 (bör genomföras inom 2–4 år)

10. Det bör föreskrivas en skyldighet för de myndigheter som ansvarar för utarbetandet av informationssäkerhetskrav att av Cybersäkerhetscentret vid Transport- och kommunikationsverket begära ett utlåtande om informationssäkerhetskrav innan kraven godkänns och vid behov även ett utlåtande om genomförandet av kraven.

Ansvarig aktör: KM, ANM, JSM, SHM, FM

Resurskonsekvenser: Kräver ytterligare finansiering.

Tidsplan för åtgärden: Angelägenhetsgrad 1 (bör genomföras inom 1–2 år från det att man avtalat om finansieringen)

11. Cybersäkerhetscentret vid Transport- och kommunikationsverket, Informationshanteringsnämnden och dataombudsmannen bör utarbeta anvisningar om allmänna aspekter som ska beaktas i informationssäkerhetskraven.

Ansvarig aktör: Transport- och kommunikationsverket, Informationshanteringsnämnden, Dataombudsmannens byrå

Resurskonsekvenser: Kräver ytterligare finansiering.

Tidsplan för åtgärden: Angelägenhetsgrad 1 (bör genomföras inom 1–2 år från det att man avtalat om finansieringen)

2.3 Kritiska funktioners och systems överensstämmelse med kraven bör utvärderas regelbundet

12. Det bör föreskrivas en skyldighet för kritiska sektorer att fastställa vilka informations- och kommunikationstekniska processer och funktioner som är kritiska. Vid fastställandet bör de särskilt beakta hur kritiska de uppgifter och det informationsmaterial som behandlas i processerna och funktionerna är liksom hur kritiska de informationssystem som används är samt processernas och funktionernas betydelse för samhällets centrala funktioner, för känsliga personuppgifter och för nationella säkerhet. Det bör i lag anges ramvillkor för när processer och funktioner ska anses vara kritiska. Vid fastställandet bör sektorerna även beakta det arbete som görs inom EU för att identifiera kritiska funktioner och kritisk infrastruktur. Vid fastställandet bör de ekonomiska konsekvenserna beaktas.

Ansvarig aktör: KM, ANM, JSM, SHM, FM

Resurskonsekvenser: Lagberedning som tjänsteuppdrag inom ramen för de nuvarande resurserna med undantag av FM där behovet är 0,5 årsverken, den nya regleringen kan medföra ytterligare resursbehov för myndigheterna.

Tidsplan för åtgärden: Angelägenhetsgrad 2 (bör genomföras inom 2–4 år)

13. Det bör föreskrivas en skyldighet för kritiska sektorer att regelbundet granska kritiska informations- och kommunikationstekniska processer och funktioner. En granskningsmodell bör fastställas i lag enligt riskerna, utgående från hur kritisk information ett system eller en process innehåller eller hur kritisk verksamhet som styrs. I granskningsmodellen bör sektorsspecifika särdrag kunna beaktas. Vid fastställandet bör de ekonomiska konsekvenserna beaktas liksom att åtgärderna är proportionerliga i förhållande till aktörernas storlek.

Ansvarig aktör: KM, ANM, JSM, SHM, FM

Resurskonsekvenser: Kräver ytterligare finansiering.

Tidsplan för åtgärden: Angelägenhetsgrad 1 (bör genomföras inom 1–2 år från det att man avtalat om finansieringen)

14. De största och de med tanke på de centrala samhällsfunktionerna viktigaste aktörerna i de kritiska sektorerna bör före slutet av 2025 kunna visa att de använder ett ledningssystem för informationssäkerhet med certifiering enligt ISO 27001 eller motsvarande certifiering som grundar sig på den allmänna standarden för informationssäkerhet. De berörda aktörerna bör fastställas separat för varje sektor i samband med genomförandet av åtgärden.

Ansvarig aktör: Sektorer som fastställts i NIS-direktivet

Resurskonsekvenser: Kräver ytterligare finansiering.

Tidsplan för åtgärden: Angelägenhetsgrad 2 (bör genomföras inom 2–4 år från det att man avtalat om finansieringen)

15. Antalet bedömningsorgan för informationssäkerhet bör utökas genom att förfarandet för godkännande av bedömningsorgan effektiviseras och genom att lagändringar som möjliggör detta bereds. I samband med lagändringarna bör det säkerställas att den höga kvaliteten på arbetet och yrkesfärdigheten vid bedömningsorganen bevaras.

Ansvarig aktör: FM

Resurskonsekvenser: De nuvarande resurserna är tillräckliga.

Tidsplan för åtgärden: Angelägenhetsgrad 1 (bör genomföras inom 1–2 år)

2.4 De kritiska sektorernas särdrag bör identifieras och beaktas

16. Det bör föreskrivas mer exakt att informationssäkerheten utgör en del av elnätsbolagens beredskapsskyldighet och beredskapsplan.

Ansvarig aktör: ANM

Resurskonsekvenser: De nuvarande resurserna är tillräckliga.

Tidsplan för åtgärden: Angelägenhetsgrad 2 (bör genomföras inom 2–4 år)

17. Det bör säkerställas att anvisningarna om informationssäkerhetskrav för kärnkraftverk är bindande.

Resurskonsekvenser: De nuvarande resurserna är tillräckliga.

Ansvarig aktör: ANM och Strålsäkerhetscentralen (STUK)

Tidsplan för åtgärden: Angelägenhetsgrad 2 (bör genomföras inom 2–4 år)

18. Det bör säkerställas att informationssäkerheten beaktas i vattentjänstverkens beredskapsplaner inför störningssituationer. Anvisningar om informationssäkerhet för vattentjänstverken bör utarbetas, och det bör säkerställas att verken följer dem i sin verksamhet.

Ansvarig aktör: JSM

Resurskonsekvenser: Kräver ytterligare finansiering.

Tidsplan för åtgärden: Angelägenhetsgrad 1 (bör genomföras inom 1–2 år från det att man avtalat om finansieringen)

19. Lagstiftningsändringar bör göras, som säkerställer att Transport- och kommunikationsverket kan meddela föreskrifter om informationssäkerhet för alla transportformer.

Ansvarig aktör: KM

Resurskonsekvenser: De nuvarande resurserna är tillräckliga.

Tidsplan för åtgärden: Angelägenhetsgrad 2 (bör genomföras inom 2–4 år)

20. Arbetsgruppen för granskning av behoven av att ändra tvångsmedelslagen bör utreda polisens befogenheter i samband med nätbrott och noga överväga olika aspekter av frågan.

Ansvarig aktör: JM:s arbetsgrupp

Resurskonsekvenser: De nuvarande resurserna är tillräckliga.

Tidsplan för åtgärden: Inom den tidsplan som fastställts för arbetsgruppen

21. Polisens resurser för att bekämpa nätbrott bör utökas, så att polisen effektivt kan förhindra, utreda och undersöka nätbrott som riktas mot kritiska sektorer.

Ansvarig aktör: IM

Resurskonsekvenser: Kräver ytterligare finansiering.

Tidsplan för åtgärden: Angelägenhetsgrad 1 (bör genomföras inom 1–2 år från det att man avtalat om finansieringen)

22. Tillsynsmyndigheterna bör instruera aktörerna att alltid göra en brottsanmälan till polisen om kränkning av informationssäkerheten när de misstänker att det är fråga om ett brott.

Ansvarig aktör: NIS-sektorsmyndigheterna

Resurskonsekvenser: De nuvarande resurserna är tillräckliga.

Tidsplan för åtgärden: Angelägenhetsgrad 1 (bör genomföras inom 1–2 år)

23. EU:s arbete med att omvärdera NIS-direktivet bör påverkas så att den kommande lagstiftningen beaktar de aktörer som är av central betydelse ur Finlands synvinkel.

Ansvarig aktör: KM

Resurskonsekvenser: De nuvarande resurserna är tillräckliga.

Tidsplan för åtgärden: Angelägenhetsgrad 1 (bör genomföras inom 1–2 år)

2.5 Den offentliga sektorns betydelse som en kritisk sektor bör identifieras och beaktas

24. Statens center för informations- och kommunikationsteknik (Valtori) bör granska sitt system och sin process i enlighet med de anvisningar som finansministeriet utfärdade i november 2020[3]. Dessutom bör Valtori före slutet av 2021 säkerställa att de konsekvensbedömningar som gäller dataskyddet har gjorts i enlighet med den allmänna dataskyddsförordningen till den del behandlingen sannolikt innebär en stor risk för människors rättigheter och friheter.

Ansvarig aktör: Valtori och FM

Resurskonsekvenser: De nuvarande resurserna är tillräckliga.

Tidsplan för åtgärden: Angelägenhetsgrad 1 (bör genomföras inom 1–2 år)

25. Ansvaret och skyldigheterna i fråga om dataskydd och informationssäkerhet för de aktörers del som tillhandahåller statens gemensamma informations- och kommunikationstekniska tjänster bör utvärderas. Utgångspunkten bör vara att det separat för de olika gemensamma kritiska tjänsterna fastställs krav på säkerhet, dataskydd och funktionssäkerhet och att det görs en utvärdering av om tjänsterna uppfyller kraven i enlighet med kriterierna i ett godkänt utvärderingsverktyg när utvärderingsverktyg bestäms på grund av varje typ av tjänst (t.ex. kraven enligt Lag om informationshantering (906/2019), ISO 27001, nivå TL IV i Katakri).

Ansvarig aktör: FM

Resurskonsekvenser: Kräver ytterligare finansiering.

[3] Finansministeriets styrningsbrev till Valtori 20.11.2020, VN/1411/2020

Tidsplan för åtgärden: Angelägenhetsgrad 2 (bör genomföras inom 2–4 år från det att man avtalat om finansieringen)

26. Det bör göras en bedömning av vilka resurser som informationssäkerheten och dataskyddet vid Valtori kräver, och nödvändiga resurser bör avsättas utifrån denna bedömning. Resurserna bör uttryckligen användas för kompetens inom informationssäkerhet och dataskydd.

Ansvarig aktör: FM, Valtori

Resurskonsekvenser: Kräver ytterligare finansiering.

Tidsplan för åtgärden: Angelägenhetsgrad 1 (bör genomföras inom 1–2 år från det att man avtalat om finansieringen)

27. Det bör säkerställas att Informationshanteringsnämndens rekommendationer från 2020 genomförs, och detta bör ske med hjälp av de Julkri-kriterier som utarbetas inom projektet Haukka 2021 och som aktörerna i den offentliga sektorn tillämpar när de fastställer informationssäkerhetskraven för molntjänster samt när de i samband med upphandlingar bedömer nivån på informationssäkerheten hos tillhandahållare av molntjänster och färdiga produkter som baserar sig på molntjänster.

Ansvarig aktör: FM, Transport- och kommunikationsverket, Myndigheten för digitalisering och befolkningsdata

Resurskonsekvenser: De nuvarande resurserna är tillräckliga.

Tidsplan för åtgärden: Angelägenhetsgrad 1 (bör genomföras inom 1–2 år)

28. Det bör utredas hur kompetensen i fråga om informationssäkerhet och dataskydd kan förstärkas vid offentliga upphandlingar till exempel via bolaget för gemensam upphandling Hansel Ab.

Ansvarig aktör: FM

Resurskonsekvenser: De nuvarande resurserna är tillräckliga.

Tidsplan för åtgärden: Angelägenhetsgrad 1 (bör genomföras inom 1–2 år)

29. Nivån på informationssäkerheten och dataskyddet inom hälso- och sjukvården, socialvården, energiförsörjningen och vattentjänsterna i Finlands 15 största kommuner bör utredas. Vid utredningen bör Cybersäkerhetscentrets tjänst för kartläggning av informationssäkerheten, som nämns i åtgärd 4, användas.

Ansvarig aktör: FM, Transport- och kommunikationsverket

Resurskonsekvenser: Kräver ytterligare finansiering.

Tidsplan för åtgärden: Angelägenhetsgrad 1 (bör genomföras inom 1–2 år från det att man avtalat om finansieringen)

2.6 Dataskyddsbestämmelser bör möjliggöra ett effektivt ingripande vid rättskränkningar

30. Nivån på dataskyddsfärdigheterna i de kritiska sektorerna bör utredas på samma sätt som i fråga om cybersäkerheten.

Ansvarig aktör: Dataombudsmannens byrå, Försörjningsberedskapscentralen (till den del det finns en koppling till försörjningsberedskap)

Resurskonsekvenser: Kräver ytterligare finansiering.

Tidsplan för åtgärden: Angelägenhetsgrad 1 (bör genomföras inom 1–2 år från det att man avtalat om finansieringen)

31. De personuppgiftsansvariga i de kritiska sektorerna bör före slutet av 2021 säkerställa att de konsekvensbedömningar som gäller dataskyddet har gjorts i enlighet med den allmänna dataskyddsförordningen till den del behandlingen sannolikt innebär en stor risk för människors rättigheter och friheter.

Ansvarig aktör: De personuppgiftsansvariga i de kritiska sektorerna, Dataombudsmannens byrå

Resurskonsekvenser: Kräver ytterligare finansiering.

Tidsplan för åtgärden: Angelägenhetsgrad 1 (bör genomföras inom 1–2 år från det att man avtalat om finansieringen)

32. Verksamheten i de certifieringsorgan som bedömer dataskyddet bör inledas genom att effektivisera förfarandet för godkännande av certifieringsorgan.

Ansvarig aktör: Dataombudsmannens byrå

Resurskonsekvenser: Kräver ytterligare finansiering.

Tidsplan för åtgärden: Angelägenhetsgrad 1 (bör genomföras inom 1–2 år från det att man avtalat om finansieringen)

33. Certifieringsorganen bör utforma kriterier för dataskyddscertifiering och lägga fram dem för dataombudsmannen för godkännande. I arbetet bör befintliga internationella standarder beaktas. Det bör göras en bedömning av om dataskyddsföreskrifter från de myndigheter som utövar tillsyn över de kritiska sektorerna eller befintliga kriterier för bedömning av dataskyddet kan godkännas som certifieringskriterier i enlighet med den allmänna dataskyddsförordningen.

Ansvarig aktör: Dataombudsmannens byrå

Resurskonsekvenser: Kräver ytterligare finansiering.

Tidsplan för åtgärden: Angelägenhetsgrad 1 (bör genomföras inom 1–2 år från det att man avtalat om finansieringen)

34. Sådana personuppgiftsansvariga i de kritiska sektorerna som behandlar uppgifter inom särskilda kategorier av personuppgifter eller uppgifter som i konstitutionellt hänseende ses som känsliga bör i stor utsträckning uppmuntras att med hjälp av dataskyddscertifiering visa att deras centrala verksamhet följer dataskyddsbestämmelserna.

Ansvarig aktör: Dataombudsmannens byrå

Resurskonsekvenser: De nuvarande resurserna är tillräckliga.

Tidsplan för åtgärden: Angelägenhetsgrad 2 (bör genomföras inom 2–4 år)

35. Det bör säkerställas att Dataombudsmannens byrå har tillräckliga resurser för att effektivt övervaka sektorerna och ingripa vid personuppgiftsincidenter. Dessutom bör man sträva efter att göra dataombudsmannens avgörandepraxis bättre tillgänglig än vad som för närvarande är fallet.

Ansvarig aktör: JM, Dataombudsmannens byrå

Resurskonsekvenser: Kräver ytterligare finansiering.

Tidsplan för åtgärden: Angelägenhetsgrad 1 (bör genomföras inom 1–2 år från det att man avtalat om finansieringen)

36. Tillämpningen av ett påföljdssystem enligt dataskyddslagen och hur väl systemet fungerar bör följas upp.

Ansvarig aktör: JM

Resurskonsekvenser: De nuvarande resurserna är tillräckliga.

Tidsplan för åtgärden: Angelägenhetsgrad 2 (bör genomföras inom 2–4 år)

2.7 Nya förfaranden för att informera om och anmäla hot mot och kränkningar av informationssäkerheten bör tas fram

37. En tjänst för privatpersoner och företrädare för organisationer bör utvecklas (t.ex. en applikation som installeras på mobila terminaler), via vilken det är möjligt att få riktad, aktuell information om hot mot och kränkningar av informationssäkerheten och om anvisningar om informationssäkerhet. Via tjänsten bör det även vara möjligt att anmäla hot mot och kränkningar av informationssäkerheten till Cybersäkerhetscentret, de myndigheter som utövar tillsyn över kritiska sektorer och polisen. Dessutom bör man via tjänsten kunna anmäla personuppgiftsincidenter till Dataombudsmannens byrå. Tjänsten (applikationen och de system som är knutna till tjänsten) bör genomföras med beaktande av principerna om säker programvaruutveckling samt god informationssäkerhet och gott dataskydd.

Ansvarig aktör: Transport- och kommunikationsverket

Resurskonsekvenser: Kräver ytterligare finansiering.

Tidsplan för åtgärden: Angelägenhetsgrad 2 (bör genomföras inom 2–4 år från det att man avtalat om finansieringen)

3 Mål och metoder

Nivån på informationssäkerheten och dataskyddet behöver utvecklas inom alla kritiska samhällssektorer. Dessutom måste skillnaderna i kunskap och kompetens mellan de olika sektorerna minskas. Det digitala samhället består av ett stort antal aktörer som är beroende av varandra.

Till exempel behöver många kritiska sektorer energiförsörjning eller kommunikationsnät för den egna sektorns grundläggande funktioner. Med tanke på kontinuiteten i samhällets verksamhet måste man säkerställa verksamhetsförutsättningarna för alla viktiga sektorer även i händelse av olika typer av störningar. När det gäller kritiska funktioner får inte en enda sektor var en svag länk.

Genom att se till att informationssäkerheten och dataskyddet är tillräckliga förstärker man även medborgarnas förtroende för det digitala samhället. I och med att personuppgifter i allt högre grad omvandlas till digital form måste medborgarna kunna lita på att uppgifterna behandlas på ett korrekt sätt och är skyddade mot dataintrång och andra rättskränkningar. Utan medborgarnas förtroende utvecklas inte de digitala tjänsterna i samhället och nyttan med digitaliseringen går förlorad.

För att uppnå målen krävs det åtgärder som får sektorsöverskridande effekter. Sådana åtgärder är till exempel en utveckling av myndighetssamarbetet och av en gemensam lägesbild, vilket kräver en förstärkning av lagstiftningen och tillräckliga resurser. För att kränkningar av informationssäkerheten och dataskyddet ska kunna förhindras och utredas bör det föreskrivas om mer etablerade samarbetsstrukturer för myndigheterna. När det gäller samarbete betonas även myndigheternas samarbete med aktörer inom den privata sektorn. Dessutom måste de expert- och informationssäkerhetstjänster som tillhandahålls av Cybersäkerhetscentret vid Transport- och kommunikationsverket i ännu högre grad bli tillgängliga för alla kritiska sektorer.

För att verksamheten ska kunna utvecklas och skillnaderna mellan de olika sektorerna minskas krävs det en heltäckande reglering och en effektiv övervakning av den. Lagstiftningen måste innehålla tillräckliga krav på informationssäkerhet och dataskydd samt bemyndiganden att meddela föreskrifter om detta, som kan kompletteras med bindande föreskrifter på längre nivå. Tidigare utredningar har visat att reglering har haft en positiv inverkan på informationssäkerheten.[4] På lagstiftningsnivå betonas dessutom fastställandet av minimikrav. Närmare sektorsspecifika informationssäkerhetskrav anges vanligen i föreskrifter eller instruktioner. För att säkerställa en tillräckligt hög nivå på informationssäkerheten och dataskyddet bör kraven grunda sig på bindande föreskrifter.

Det räcker inte att endast förstärka regleringen, utan det behövs även tillräckliga resurser för att genomföra och övervaka den och för att instruera och vägleda aktörerna. För närvarande är de resurser som avsatts för informationssäkerhet och dataskydd otillräckliga inom många kritiska samhällssektorer. Detta gäller även den sektorsspecifika myndighetstillsynen, och myndigheterna har inte ens möjlighet att använda sina befogenheter enligt lagstiftningen. För att verksamheten ska kunna utvecklas och resurserna riktas till en utveckling av informationssäkerheten och dataskyddet krävs det mod av ledningen.

Även om en effektiv myndighetstillsyn i hög grad kan anses bidra till en förbättring av informationssäkerheten och dataskyddet i samhället har varje aktör själv det primära ansvaret för informationssäkerheten och dataskyddet. Hur omfattande tillsynen än är kan den inte ensam göra samhället och de kritiska samhällsfunktionerna säkra. Utgångspunkten bör vara att informationssäkerheten och dataskyddet är integrerade i verksamhetskulturen i de kritiska sektorerna, och aktörerna måste själva ansvara för detta.

[4] Försörjningsberedskapscentralens rapport om nuläget för cybersäkerheten inom olika sektorer (på finska): https://cdn.huoltovarmuuskeskus.fi/app/uploads/2020/10/05091400/Kyberturvallisuuden-nykytila-eri-toimialoilla.pdf

Sammanfattningsvis kan det konstateras att en förbättring av informationssäkerheten och dataskyddet inom kritiska samhällssektorer kräver följande:

1. Lagstiftningen måste innehålla tillräckliga krav och skyldigheter i fråga om informationssäkerhet och dataskydd, som ska tillämpas av de olika sektorerna, liksom bestämmelser om meddelande av närmare föreskrifter om genomförandet av informationssäkerheten och dataskyddet.
2. Aktörerna måste ha tillräckliga kunskaper och färdigheter för att kunna fullgöra skyldigheterna.
3. Myndigheterna måste ha tillräckliga befogenheter att övervaka informationssäkerheten och dataskyddet samt samarbeta över sektorsgränserna.
4. Myndigheterna måste ha tillräckliga kunskaper och mod för att använda sina befogenheter enligt lagstiftningen och styra sin sektor.
5. Myndigheterna måste ha tillräckliga, faktiska materiella resurser och personalresurser för att kunna använda sina befogenheter.
6. Varje aktörer måste själv ansvara för informationssäkerheten och dataskyddet för den egna verksamheten.
7. En gemensam lägesbild av verksamhetsmiljön när det gäller informationssäkerheten och dataskyddet måste upprätthållas, vilket även inbegriper samordning, informationsutbyte och lägesrapporter.
8. Åtgärder för att stärka medborgarnas digitala säkerhetskompetens inleds som ett omfattande samarbete mellan olika aktörer.

4 Bedömning av nuläget

Riktlinjerna i principbeslutet utgår från nuläget, som behandlades ingående i slutrapporten från den tväradministrativa arbetsgrupp som utrett en förbättring av informationssäkerheten och dataskyddet inom kritiska sektorer i samhället[5]. De viktigaste observationerna om nuläget sammanfattas nedan:

1. I Finland fördelas ansvaret för myndighetstillsynen över informationssäkerheten och dataskyddet mellan flera olika myndigheter. I de sektorer som är kritiska med tanke på informationssäkerheten ansvarar sektorsmyndigheterna vid sidan av annan tillsyn även för tillsynen över informationssäkerheten i den egna sektorn. Dataombudsmannens byrå övervakar att dataskyddslagstiftningen och andra lagar som gäller behandling av personuppgifter följs. Polisen ansvarar för brottsutredningar.

2. Cybersäkerhetscentret vid Transport- och kommunikationsverket har egna sektorsspecifika tillsynsuppgifter och ger därtill direkt stöd till aktörer inom de olika samhällssektorerna. För att Cybersäkerhetscentret ska kunna ge tillräckligt stöd till de olika sektorerna måste det vid centret finnas tillräckliga kunskaper om sektorernas verksamhet och om verksamhetsmiljön. Tillräckliga resurser måste avsättas för verksamheten så att lägesbilden kan hållas uppdaterad och analyseras med beaktande av de enskilda sektorernas behov. Med nuvarande resurser kan Cybersäkerhetcentret inte erbjuda alla kritiska samhällssektorer tillräckliga tjänster.

[5]Förbättring av informationssäkerheten och dataskyddet inom kritiska sektorer i samhället: Arbetsgruppens slutrapport (Kommunikationsministeriets publikationer 1/2021), http://urn.fi/URN:ISBN:978-952-243-614-6).

3. Utgångspunkten för samarbetet mellan myndigheter är att de myndigheter som ansvarar för informationssäkerheten måste samarbeta när deras uppgifter så kräver. Även NIS-direktivet förutsätter att de myndigheter som ansvarar för informationssäkerheten samarbetar i den omfattning som krävs för att de ska kunna övervaka skyldigheterna enligt direktivet. Utanför NIS-direktivets tillämpningsområde sker myndighetssamarbete till exempel vid brottsutredningar. I fallet med psykoterapicentret Vastaamo var behöriga myndigheter utöver polisen åtminstone Valvira, regionförvaltningsverken, dataombudsmannen och Transport- och kommunikationsverket.

4. Myndighetssamarbete bör alltid föreskrivas i lag när det är fråga om handräckning där man ingriper i ett enskilt rättssubjekts i grundlagen skyddade rättigheter eller när det är fråga om utövning av offentlig makt enligt grundlagen. Även informationsutbyte i samband med myndighetssamarbete kan kräva reglering på lagnivå. Om det för ett myndighetssamarbete inrättas ett samarbetsorgan med beslutanderätt måste även detta föreskrivas i lag. Det kan dessutom vara lämpligt att föreskriva om myndighetssamarbete även om det juridiskt sett inte är nödvändigt. Särskilda bestämmelser om samarbete på lagnivå betonar vikten av samarbetet för de myndigheter som deltar i det och kan bidra till organiserade former för samarbetet. En effektivisering av myndighetssamarbetet har setts som en viktig metod att förbättra informationssäkerheten och dataskyddet.

5. Det finns stora skillnader mellan de kritiska samhällssektorerna när det gäller hur noggranna krav på informationssäkerhet och dataskydd som har föreskrivits med stöd av lag. Både de myndigheter som övervakar informationssäkerheten och de aktörer som gör informationssäkerhetsbedömningar har lyft fram behovet av mer detaljerade krav på informationssäkerhet. Framför allt inom sektorerna för energi, transporter och vattentjänster har det utfärdats få eller inga krav med stöd av lag. I vissa fall finns det inte bemyndiganden i lag att utfärda bestämmelser på lägre nivå eller så har bemyndigandena inte utnyttjats. En motsvarande situation förekommer inom informationshanteringen i den offentliga sektorn, särskilt när det gäller bestämmelser på lägre nivå.

6. Endast en del av aktörerna inom de kritiska samhällssektorerna beställer revisionstjänster eller certifikat som gäller den egna informationssäkerheten. Det låga utnyttjandet av revisioner inom vissa sektorer har bidragit till att nivån på informationssäkerheten för processer, funktioner och informationssystem kan variera kraftigt mellan olika sektorer. Revision av processer och funktioner borde vara en naturlig del av riskhanteringen inom kritiska sektorer.

5 Behov av ytterligare resurser

I samband med beredningen av principbeslutet bedömdes vilka konkreta ytterligare resurser som behövs inom de olika förvaltningsområdena för att sektorsmyndigheterna effektivt ska kunna övervaka informationssäkerheten. Vid bedömningen beaktade man den tväradministrativa arbetsgruppens tidigare bedömningar av behovet av ytterligare resurser. De sektorer som granskades var i enlighet med NIS-direktivet framför allt hälso- och sjukvården, finansmarknaden, energiförsörjning, vattentjänster, transporter och digital infrastruktur samt kommunikationsnät. Dessutom granskades viktiga informationssystem inom staten och kommunerna, och i fråga om ytterligare resurser granskades i synnerhet de bedömningar som gällde statens system. Slutligen granskades även polisens resurser, framför allt med tanke på kampen mot nätbrott. Arbetsgruppen granskade inte säkerhetsmyndigheternas nätverk och system eftersom man ansåg att sådana mycket säkerhetskritiska funktioner bör granskas separat.

Enligt den bedömning som gjordes i samband med beredningen av principbeslutet behövs det inom de nämnda sektorerna sammanlagt ytterligare 115 årsverken inom myndighetsfunktioner

för att riktlinjerna i principbeslutet ska kunna genomföras och för att tillsynen, styrningen och rådgivningen i fråga om informationssäkerhet och dataskydd ska kunna höjas till den nivå som krävs. Bedömningen inbegriper även de ytterligare sex årsverken som föreslagits för kommunikationsministeriet i syfte att säkerställa att resurserna är tillräckliga för att motsvara den ökande arbetsmängd som cybersäkerheten medför och cybersäkerhetens betydelse i samhället. Kostnaderna för dessa ytterligare årsverken bedöms uppgå till sammanlagt cirka 10,2 miljoner euro per år. Dessutom har man uppskattat att det inom förvaltningsområdena uppstår bland annat IKT-systemkostnader och upphandlingskostnader, vars storleksklass kan variera kraftigt beroende på metoden och tidpunkten för implementeringen.

Man har gjort en indelning av riktlinjerna i principbeslutet där man utgår från om det behövs ytterligare resurser ur statsbudgeten eller om de nuvarande resurserna i huvudsak är tillräckliga. Bedömningen är att riktlinjerna 1, 8, 9, 12, 15, 16, 17, 19, 20, 22, 23, 24, 27, 28, 34 och 36 kan genomföras inom ramen för de nuvarande resurserna. Även dessa åtgärder kan dock få indirekta resurskonsekvenser för myndigheternas verksamhet, till exempel till följd av ändringar i lagstiftningen. Riktlinjerna 2, 3, 4, 5, 6, 7, 10, 11, 13, 14,18, 21, 25, 26, 29, 30, 31, 32, 33, 35 och 37 kräver ytterligare finansiering, och kan således inte genomföras inom ramen för de nuvarande resurserna.

Avsikten är att både riktlinjerna och de resurser som avsätts för dem ska stödja varandra och att de bör granskas som en helhet. Detta innebär att effekten av en enskild åtgärd ofta är beroende av genomförandet av de andra åtgärder som föreslås.

Riktlinjerna i principbeslutet genomförs inom ramen för statsbudgeten och de nuvarande resurserna. De ytterligare föreslagna resursbehoven eller andra åtgärder som har budgetkonsekvenser kommer att avgöras separat inom ramen för statsekonomin och i årliga budgetarna. De ytterligare resursbehov som presenterades i detta principbeslut är således villkorliga och kan bara genomföras om den totala finansieringen för förbättringen av informationssäkerheten och dataskyddet ökas i olika förvaltningsområden genom budgetresurser. Detta måste beslutas och avtalas separat.

6 Uppföljning och rapportering

Kommunikationsministeriet ansvarar för att följa upp genomförandet av riktlinjerna i principbeslutet i samarbete med de aktörer som nämns i samband med åtgärderna, och dessutom förstärks kommunikationsministeriets samordnande roll vid hanteringen av plötsliga och exceptionella informationssäkerhets- och dataskyddsincidenter. De aktörer som enligt riktlinjerna är ansvariga ska rapportera till kommunikationsministeriet om hur åtgärden framskrider. För varje åtgärd har det fastställts en angelägenhetsgrad som anger inom vilken tidsperiod åtgärden bör genomföras.