Cybersäkerhet

Anvisning för aktörer inom social- och hälsovården

SOCIAL- OCH HÄLSOVÅRDSMINISTERIETS PUBLIKATIONER 2019:17

Social- och hälsovårdsministeriets publikationer 2019:17

Cybersäkerhet

Anvisning för aktörer inom social- och hälsovården

Social- och hälsovårdsministeriet, Helsingfors 2019

Social- och hälsovårdsministeriet

ISBN PDF: 978-952-00-4092-5

Layout: Statsrådets förvaltningsenhen, publikationsverksamheten

Helsingfors 2019

Presentationsblad

Utgivare	Social- och hälsovårdsministeriet		23.5.2019
Författare	Sari Vuorinen (redaktör)		
Publikationens titel	Cybersäkerhet Anvisning för aktörer inom social- och hälsovården		
Publikationsseriens namn och nummer	Social- och hälsovårdsministeriets publikationer 2019:17		
Diarie-/ projektnummer	5500H-VAL.0603	**Tema**	
ISBN PDF	978-952-00-4092-5	**ISSN PDF**	1797-9854
URN-adress	http://urn.fi/URN:ISBN:978-952-00-4092-5		
Sidantal	62	**Språk**	svenska
Nyckelord	social- och hälsovård, cybersäkerhet, samhällets vitala funktioner, övergripande säkerhet, beredskapsplanering, beredskap		

Referat

Cybersäkerheten är en del av beredskapen inom social- och hälsovårdstjänsterna.

Syftet med anvisningen är att ge en allmän bild av principerna för cybersäkerhet som gäller branschen samt förefintliga anvisningar och rekommendationer. Anvisningen baserar sig på verkställighetsprogrammet för Finlands cybersäkerhetsstrategi och den stöder för sin del säkerställandet av samhällets vitala funktioner i störningssituationer.

Anvisningen presenterar inte detaljerade eller tekniska åtgärder för identifiering eller bekämpning av cyberhot, utan för detta får aktörerna handledning från bland annat Cybersäkerhetscentret. Dessutom har till exempel Institutet för hälsa och välfärd producerat definitioner, bestämmelser och utbildningsmaterial för informationshanteringen inom branschen.

Anvisningen är avsedd som en allmän anvisning för aktörer inom social- och hälsovården i olika organisationer och den har beretts i ett projekt som är gemensamt för social-och hälsovårdsministeriet och Kommunförbundet.

Den första versionen av denna anvisning kommer att publiceras i social- och hälsovårdsministeriets publikationsserie och den kommer att uppdateras enligt behov. Som bilagor finns information som ger bakgrunden och fördjupande information.

Förläggare	Social- och hälsovårdsministeriet
Distribution/ beställningar	Elektronisk version: julkaisut.valtioneuvosto.fi Beställningar: julkaisutilaukset.valtioneuvosto.fi

Kuvailulehti

Julkaisija	Sosiaali- ja terveysministeriö		23.5.2019
Tekijät	Sari Vuorinen (toimittaja)		
Julkaisun nimi	Kyberturvallisuus Ohje sosiaali- ja terveydenhuollon toimijoille		
Julkaisusarjan nimi ja numero	Sosiaali- ja terveysministeriön julkaisuja 2019:17		
Diaari/hankenumero	5500H-VAL.0603	**Teema**	
ISBN PDF	978-952-00-4092-5	**ISSN PDF**	1797-9854
URN-osoite	http://urn.fi/URN:ISBN:978-952-00-4092-5		
Sivumäärä	62	**Kieli**	ruotsi
Asiasanat	sosiaali- ja terveydenhuolto, kyberturvallisuus, yhteiskunnan elintärkeät toiminnot, valmius, kokonaisturvallisuus, valmiussuunnittelu, varautuminen		

Tiivistelmä

Kyberturvallisuus on osa sosiaali- ja terveydenhuollon palveluiden valmiutta ja varautumista.

Ohjeen tarkoitus on antaa yleiskuva toimialaa koskevista kyberturvallisuuden periaatteista sekä olemassa olevista ohjeista ja suosituksista. Ohje perustuu Suomen kyberturvallisuusstrategian toimeenpano-ohjelmaan ja sillä tuetaan osaltaan yhteiskunnan elintärkeiden toimintojen varmistamista häiriötilanteissa.

Ohje ei esitä yksityiskohtaisia tai teknisiä toimenpiteitä kyberuhkan tunnistamiseen tai torjuntaan, vaan niitä varten toimijat saavat ohjausta muun muassa Kyberturvallisuuskeskukselta. Lisäksi esimerkiksi Terveyden ja hyvinvoinnin laitos on tuottanut määrittelyjä, määräyksiä ja koulutusmateriaalia toimialan tiedonhallintaan.

Ohje on tarkoitettu yleisohjeeksi sosiaali- ja terveydenhuollon toimijoille erilaisissa organisaatioissa ja se on valmisteltu sosiaali- ja terveysministeriön ja Kuntaliiton yhteisessä hankkeessa.

Tämän ohjeen ensimmäinen versio julkaistaan sosiaali- ja terveysministeriön julkaisusarjassa ja sitä tullaan päivittämään tarpeiden mukaan. Liitteinä on taustoittavaa ja syventävää tietoa.

Kustantaja	Sosiaali- ja terveysministeriö
Julkaisun jakaja/ myynti	Sähköinen versio: julkaisut.valtioneuvosto.fi Julkaisumyynti: julkaisutilaukset.valtioneuvosto.fi

Description sheet

Published by	Ministry of Social Affairs and Health		23rd May 2019
Authors	Sari Vuorinen (Editor)		
Title of publication	Cyber security Guidance for operators in the healthcare and social welfare sectors		
Series and publication number	Publications of the Ministry of Social Affairs and Health 2019:17		
Register number	5500H-VAL.0603	**Subject**	
ISBN PDF	978-952-00-4092-5	**ISSN (PDF)**	1797-9854
Website address (URN)	http://urn.fi/URN:ISBN:978-952-00-4092-5		
Pages	62	**Language**	Swedish
Keywords	social welfare and health care, cyber security, vital functions of society, readiness, comprehensive security, contingency planning, preparedness		

Abstract

Cyber security is part of preparedness and contingency planning in social welfare and healthcare services.

The purpose of the guidance document is to provide a general overview of the cyber security principles applicable to the sector and to introduce existing guidelines and recommendations. The guidance document is based on the implementation programme of Finland's Cyber Security Strategy, and it helps to secure the vital functions of society in abnormal conditions.

It does not provide detailed or technical measures for identifying or combating cyber threats; guidance for these is provided by agencies such as the National Cyber Security Centre. In addition, the National Institute for Health and Welfare has produced specifications, orders and training material for the sector's information management purposes.

The guidance document is intended as a general guideline for social welfare and health care operators in various organisations, and it has been jointly prepared by the Ministry of Social Affairs and Health and the Association of Finnish Local and Regional Authorities.

The first version of this document is published in a publication series of the Ministry of Social Affairs and Health, and it will be updated as and when necessary. More detailed background information is provided in the appended documents.

Publisher	Ministry of Social Affairs and Health
Distributed by/ publication sales	Online version: julkaisut.valtioneuvosto.fi Publication sales: julkaisutilaukset.valtioneuvosto.fi

Innehåll

TILL LÄSAREN

Med övergripande säkerhet avses en samverkansmodell för den finländska beredskapen där myndigheterna, näringslivet, organisationerna och medborgarna tillsammans ser till samhällets vitala funktioner. Social- och hälsovården har en högst betydande roll i denna beredskap. I olika störningssituationer uppstår det i praktiken alltid uppgifter för socialvården, hälso- och sjukvården samt miljö- och hälsoskyddet.

Modellen för övergripande säkerhet förutsätter att beredskapen i branschen grundar sig på enhetliga riskbedömningar och planering. På så sätt säkerställs funktionsförmågan i olika störningssituationer på det nationella, regionala och lokala planet och i samarbetet med andra aktörer.

Beredskapen för cyberstörningssituationer och hanteringen av dessa ingår i social- och hälsovårdsorganisationernas dagliga arbete och kontinuitetshantering.

Jag hoppas att denna anvisning om cybersäkerhet bidrar med effektiva praktiska rekommendationer och metoder för social- och hälsovårdsaktörerna i detta viktiga arbete.

För att harmonisera och stödja beredskapsplaneringen inom social- och hälsovården utges även andra relaterade anvisningar, till exempel om kontinuitetshantering (Kuja-modellen) och avtalsbaserad beredskap.

Helsingfors maj 2019

Kanslichef Päivi Sillanaukee

Rekommendationer

- Beredskapen för cyberstörningssituationer och hanteringen av dessa ska ingå i social- och hälsovårdsorganisationernas dagliga arbete (hotens frekvens).
- Cybersäkerhet ska beaktas som en del av tjänsteproduktionen inom all resursfördelning och även vid upphandlingen av system och tjänster (ledningens roll).
- Social- och hälsovårdsorganisationer ska med tanke på sin beredskap definiera de egna kritiska funktionerna samt de producerade tjänsterna och relaterade kritiska systemen, såsom utrustning och program, som ska säkerställas i alla situationer (definition av kritiska funktioner).
- Säkerheten och beredskapen inför störningssituationer ökar oundvikligen kostnaderna. I fråga om den kritiska verksamheten ska en sådan kapacitet säkerställas som krävs för att klara av störningssituationer. Kritiska system ska kunna upprätthållas enligt tillverkarens direktiv och nödvändiga programuppdateringar göras utan att den normala verksamheten störs (upprätthållande av kritiska funktioner).
- Kunskap om informationssäkerhet och dataskydd är en viktig del av social- och hälsovårdspersonalens yrkeskunskap (var och ens ansvar).
- Alla anställda ska veta hur man går till väga om informationssystemen inte fungerar normalt. Alternativa handlingssätt ska övas. Personalens kunskap om informationssäkerhet ska säkerställas regelbundet (utbildning och övning).
- Samarbetet mellan olika aktörer ska fastställas på förhand och övas (modell för hantering av störningssituationer).

Inledning

Anvisningen om cybersäkerhet för social- och hälsovårdsaktörer har utarbetats inom projektet för beredskap och kontinuitetshantering inom vårdstrukturerna, som är social- och hälsovårdsministeriets och Finlands Kommunförbunds gemensamma projekt. Anvisningen grundar sig på verkställighetsprogrammet för strategin för cybersäkerhet i Finland 2011–2017.

Cybersäkerhet ingår i säkerställandet av social- och hälsovårdens tjänster och den övergripande säkerheten. Social- och hälsovården utsätts för cyberhot varje dag. Denna anvisning bidrar till att upprätthålla och säkerställa samhällets vitala funktioner under normala förhållanden och i störningssituationer.

Anvisningen syftar till att ge en överblick över de principer om cybersäkerhet som gäller social- och hälsovården samt de befintliga anvisningarna och rekommendationerna. Denna information behövs i styrningen, upphandlingen och produktionen av social- och hälsovårdstjänster, varför anvisningen riktar sig till alla dem som arbetar inom social- och hälsovårdens förvaltning och praktiska verksamhet.

Anvisningen är inte avsedd att ge detaljerade tekniska lösningar för att förbättra cybersäkerheten. För detta ändamål finns separat material som tagits fram av bland annat Cybersäkerhetscentret. Med hjälp av cybersäkerhet tryggas kvaliteten och effektiviteten i vården och servicen inom social- och hälsovården. Informationssäkerhet och dataskydd är en permanent del av denna helhet, varför även informationssäkerhets- och dataskyddsfrågor tas upp i anvisningen.

I den arbetsgrupp som utarbetat cybersäkerhetsanvisningen företräddes de främsta experterna inom cybersäkerhet. Arbetsgruppen bestod av Lasse Ilkka, ordförande (social- och hälsovårdsministeriet), Perttu Halonen (Traficom, Cybersäkerhetscentret), Jani Jussila (Finlands Kommunförbund), Maritta Korhonen (FPA), Tuija Kuusisto (finansministeriet), Andrei Laurén (Institutet för hälsa och välfärd), Kalle Luukkainen (Försörjningsberedskapscentralen), Jaakko Pentti (SoteDigi Oy), Maarit Puhto (social- och hälsovårdsministeriet), Jussi Rapeli (Egentliga Finlands sjukvårdsdistrikt), Jarkko Reittu (Institutet för

hälsa och välfärd), Kimmo Rousku (Befolkningsregistercentralen), Jenni Siermala (Norra Österbottens sjukvårdsdistrikt, SoteDigi Oy fr.o.m. 3.1.2019), Veijo Terho (ICT-palvelukeskus Vimana Oy), Teemupekka Virtanen (social- och hälsovårdsministeriet) och Sari Vuorinen, sekreterare (Finlands Kommunförbund).

I beredningen av anvisningen har man även samarbetat med andra sakkunniga, till exempel inom ramen för Försörjningsberedskapscentralens projekt om cyberhälsa. Tack till alla som deltagit i beredningen.

Anvisningen om cybersäkerhet ges ut endast i elektronisk form och kommer att uppdateras som ett led i styrningen av den nationella beredskapsplaneringen.

Social- och hälsovårdens verksamhetsmiljö

Social- och hälsovårdspersonalen använder dagligen digitala tjänster i sitt arbete. Vid genomförandet av tjänsterna utnyttjas i väsentlig grad informations- och kommunikationsteknik, såsom mobil teknik, molntjänster, artificiell intelligens, IoT (Internet of things) och ICMT[1] (Information, Communication and Medical Technology). Den snabba tekniska utvecklingen innebär allt fler utmaningar när det gäller att producera tjänster på ett datasäkert och standardenligt sätt. Störningssituationer i anslutning till informationssystem har under de senaste åren allt oftare lyfts fram i offentligheten, till exempel i samband med Olycksutredningscentralens utredning av de allvarliga datastörningarna i Helsingfors och Nylands sjukvårdsdistrikt 7–8.11.2017[2].

Finland hör till föregångarna i världen när det gäller att utnyttja digital teknik. En stor mängd uppgifter samlas in, men den nationella samkörningen och utnyttjandet av dem bör utvecklas. De yrkesutbildade personerna i branschen ska ha digital tillgång till de uppgifter som behövs i det dagliga klient- och patientarbetet. Även medborgarna kommer i allt högre grad åt sina egna hälso- och välfärdsuppgifter. Med hjälp av dem kan medborgarna bedöma sin egen hälsa och få information om vilka tjänster som motsvarar deras behov och hur de själva kan förbättra sin livssituation.

Inom social- och hälsovården ska särskild uppmärksamhet fästas vid behandlingen av klient- och personuppgifter på grund av uppgifternas känsliga natur. Uppgifternas konfidentialitet ska skyddas för att garantera integriteten. Detta fastställs genom lagstiftning men det är även fråga om hälso- och sjukvårdens rykte och trovärdighet vid behandlingen av känsliga hälsouppgifter.

Förutom att känsliga uppgifter är sekretessbelagda är också uppgifternas integritet och tillgänglighet högst relevanta ur ett säkerhetsperspektiv. Patientens vård och klientens

1 ICMT = Information, Communication and Medical Technology. Termen används vid hänvisning till såväl datateknik som medicinteknisk utrustning.

2 https://www.turvallisuustutkinta.fi/sv/index/ajankohtaista/tiedotteet/2019/01/turvallisuustutkintahelsinginjauudenmaansairaanhoitopiirintietojarjestelmienvakavistahairioista7.-8.11.2017valmis-terveydenhuollontietojarjestelmattuleepitaakunnossa.html

service grundar sig på uppgifter som ska vara korrekta och kunna hänföras till rätt patient. Uppgifterna ska kunna användas precis då de behövs.

Social- och hälsovårdstjänster produceras i allt högre grad även i patientens och klientens hemmamiljö. Genom att använda informationssystem inom social- och hälsovården strävar man i sista hand efter fördelar för patienterna och klienterna: högklassig och effektiv vård och service. Cybersäkerheten ökar informationsbehandlingens konfidentialitet.

I tekniskt avseende kräver användningen av tjänsterna även digitala tjänster av tredje parter, såsom elektroniska identifieringstjänster.

Hälso- och sjukvårdens informationssystem

Hälso- och sjukvårdens nationella informationsarkitektur består av lokala, regionala och nationella system. De lokala och regionala systemen utgörs av de egentliga operativa system som används dagligen, medan de nationella systemen används för att lagra och distribuera information.

Ett typiskt lokalt system är patientdatasystemet som används av personalen för att hantera patientuppgifter och det egna dagliga arbetet. Centrala nationella system är till exempel det nationella patientdataarkivet (Kanta) och kodtjänsten. Kanta-tjänsterna är avsedda både för social- och hälsovårdproffsen och för medborgarna. Kanta-tjänsterna omfattar exempelvis patientdataarkivet, elektroniska recept och möjligheten att kontrollera sina egna hälsouppgifter via nätet (Mina Kanta-sidor).

Inom hälso- och sjukvården förutsätter användningen av patientuppgifter att vårdande personen har en vårdrelation till patienten. Den yrkesutbildade person som har hand om vården har rätt att se patientjournalen och skyldighet att spara sina egna logguppgifter i den. Varje person som deltar i vården har rätt att se de uppgifter som krävs för det egna deltagandet. Utlämnandet av uppgifter mellan personuppgiftsansvariga grundar sig på patientens samtycken och förbud. Patienten kan förbjuda att hans eller hennes uppgifter är synliga för en annan personuppgiftsansvarig.

Hälso- och sjukvårdsproducenterna har kopplat sina patientdatasystem till de nationella tjänsterna. De kan använda de kodverk som laddats ned från kodtjänsten samt söka och uppdatera patientdata i Kanta-tjänsten. Inom hälso- och sjukvården följs patientens situation upp med hjälp av en fortlöpande patientjournal som bildas av separata patientjournaler.

Den nationella arkitekturen grundar sig på att det finns en centraliserad lagringsplats, där man via samtliga lokala och regionala patientdatasystem kan lagra väsentliga patientuppgifter. Patientuppgifterna i Kanta-tjänsten kan lämnas ut till lokala system om inte patienten förbjudit detta. I de regionala systemen kan de patientuppgifter som den egna personuppgiftsansvariga samlat in användas även utan en anslutning till Kanta-tjänsten. De informationssystem som ansluts till Kanta-tjänsterna ska genomgå en certifieringsprocess som bland annat inkluderar en datasäkerhetsauditering.

Inom det nationella systemet har man satsat avsevärt på skyddet och övervakningen av datakommunikationen. Största delen av datakommunikationen mellan systemen sker i separata nätverk. En del av de mindre aktörerna i branschen använder tjänster via det offentliga nätet, vilket gör dem sårbara för olika störningar i detta. Till exempel tjänsten Mina Kanta-sidor fungerar via det offentliga nätet. Det är inte fråga om ett kritiskt system för samhället men det är synligt och utsatt. Dessutom behandlar hälso- och sjukvårdsklienterna sina egna uppgifter med egen utrustning i egen miljö, varvid känsliga uppgifter kan läcka ut i offentligheten som en följd av klienternas eget agerande.

De cyberattacker som riktats mot detta system har i allmänhet skett antingen inom det offentliga nätet eller i de lokala systemen, varvid de inte nämnvärt påverkat de nationella tjänsterna. Genom utomstående attacker har man bland annat stört verksamheten på Mina Kanta-sidor och hos de tjänsteleverantörer som använder det offentliga nätet. Attackerna i sig har varit typiska överbelastningsattacker, vilka antingen riktats direkt mot Kanta-tjänsterna eller mot de kritiska tjänsterna på nätet, såsom Befolkningsregistercentralens tjänster.

Sjukhusmiljöns särdrag

Sjukhusen utgör en central verksamhetsmiljö för hälso- och sjukvårdens informationssystem. Inom hälso- och sjukvården används i allt högre grad sakernas internet (IoT, Internet of Things).

De medicintekniska produkterna på sjukhusen är allt oftare kopplade till internet, sjukhusens informationsnät och annan utrustning, vilket i sig ökar informationssäkerhetsriskerna. Dessa risker har blivit vanligare och vardagligare i takt med den tekniska utvecklingen och människornas användningsvanor. En ytterligare utmaning är att kraven på cybersäkerhet inte ännu i tillräcklig grad beaktas i de medicintekniska produkternas godkännandekriterier.

Med hjälp av utrustning som kopplas upp till internet eller annan utrustning kan man ta nya och effektivare vårdmetoder i bruk i sjukhusmiljöerna, hos hälso- och

sjukvårdsaktörerna och i hemmavården. I takt med att sjukhusen blir allt intelligentare begränsas deras verksamhet inte längre enbart till sjukhusmiljön. Det är nödvändigt att ta hänsyn till alla olika verksamhetsmiljöer där man eventuellt använder utrustningen, applikationerna och delar av dessa.

Ett sjukhus behöver ett stort antal stödtjänster för att fungera. En stor mängd aktörer och stödtjänster är direkt eller indirekt knutna till patientens vård. Med tanke på vårdens kontinuitet måste stödtjänsterna fungera även i störningssituationer. Till sjukhusets cybermiljö hör också vanlig kontorsdatateknik. Om det till exempel uppstår störningar i sjukhusets betalningstrafik påverkar det faktureringen av patienternas sjukhus-/hälsovårdscentralsavgifter, utbetalningen av personalens löner samt betalningen av köpfakturor för medicin- och vårdutrustning till leverantörerna.

I figuren nedan beskrivs en typisk verksamhetsmiljö inom hälso- och sjukvården, där patientens vård inklusive de väsentliga laboratorie- och bilddiagnostiktjänsterna står i centrum.

Figur 1. Hälso- och sjukvårdens verksamhetsmiljö (Källa: Poolen för hälsovård)

Inom hälso- och sjukvården ska man utöver patientdata ta hänsyn även till andra cybersäkerhetsaspekter. Delområden av ett smart sjukhus[3] är exempelvis:

- Distansvårdssystem med vilka man kan följa upp patientens tillstånd eller rentav utföra vårdåtgärder, såsom att distribuera mediciner.
- Medicinteknisk utrustning som är kopplad till nätet, t.ex. bärbara datorer, påklädbar teknik eller assisterande robotar.
- System för att identifiera patienter, såsom olika smarta armband eller biometriska skannrar.
- Nätutrustning för att koppla upp den ovannämnda fjärrutrustningen till sjukhusets system.
- Mobila apparater inklusive applikationer med vilka vårdpersonalen bär med sig nödvändig information.
- Huvudsakliga informationssystem för klinisk vård i vilka patientdata lagras och behandlas.
- Själva informationsinnehållet som kan bestå av både kliniska patientdata och forskningsdata, uppgifter om personalen eller information om sjukhusets verksamhet.
- Fastighetsautomatik i sjukhusbyggnader som stöder verksamheten i intelligenta sjukhus, såsom automatiska dörrar och smartlås, intelligenta VVS- och elektriska system och automatiska system för vårdrum eller produktion av ånga för sterilisering av instrument.

Socialvårdens informationssystem

Socialvårdens cybermiljö består utöver vanlig kontorsdatateknik av de informationssystem som huvudsakligen används för att behandla socialvårdens klientdata samt av anslutningsgränssnitt och datanät mellan dessa. Den behandlade informationen kan bestå av vanliga personuppgifter eller känsliga klientdata i anslutning till socialvårdens tjänster som ska skyddas särskilt noga. I klientdatasystemen fattas även myndighetsbeslut och det görs betalningar och ingås betalningsförbindelser med tjänsteproducenter. Till socialvårdens omgivning hör fastighetssystem, såsom övervaknings- och överfallssystem.

Inom socialvården har man börjat ta nationella informationssystemstjänster i bruk för klientdata och nationella klientdatalager. Klientdataarkivet för socialvården är ett nationellt informationssystem som möjliggör centraliserad elektronisk arkivering av socialvårdens klientdata samt aktiv användning av och permanent lagring av uppgifterna. Tjänsten kan tas i bruk av de socialvårdsproducenter som lagrar klienthandlingar elektroniskt.

3 Publikation om cyberhot på intelligenta sjukhus av EU:s nätverks- och informationssäkerhetsbyrå (ENISA) 2016 https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals

Arkivet används med hjälp av ett system för hantering av socialvårdens klientdata och användningen förutsätter registrering i Kanta-tjänsterna. Inom projektet Kansa utvecklas socialvårdstjänsterna under 2016–2020, bland annat klientdataarkivet för socialvården som en del av Kanta-tjänsterna.

Hoten inom socialvården hänför sig för närvarande främst till att utomstående ska komma över klienternas uppgifter. Om klientdatasystemen inte fungerar ska socialvården med hjälp av reservsystem garantera mat och inkvartering för personer som har det sämst ställt samt nödvändig omsorg för anstaltboende (funktionshindrade, barnskyddet, enheter för stödboende, äldrevården, mentalvårds- och missbruksklienter). Störningar i betalningstrafiken påverkar socialvårdens klienter. Störningarna kan försvåra betalningen av socialtrygghetsstöd och därigenom försämra människornas utkomstskydd. Det kan också vara fråga om en strävan efter ekonomisk vinning. Man kanske försöker manipulera uppgifterna i informationssystemen så att de gynnar sökanden, ändra betalningsuppgifterna för att styra pengarna till fel part eller skapa ogrundade betalningar.

Socialvårdstjänster produceras i allt högre grad även i patienternas och klienternas hemmamiljö. I störningssituationer ska tjänsterna för de klienter som är beroende av service i hemmet tryggas. Genom cybersäkerhet strävar man inom socialvården efter att garantera patienterna och klienterna bra vård samt högklassig och effektiv service. I tekniskt avseende kräver användningen av tjänsterna även digitala tjänster av tredje parter, såsom elektroniska identifieringstjänster.

Cyberhot mot social- och hälsovården

Cyberbrottslingar har särskilt under 2016–2018 favoriserat utpressningsprogram för kryptering av filer (crypto ransomware). Dessa skadliga program infekterar offrets dator och krypterar filerna på den. Brottslingarna kräver sedan att offren betalar lösen mot en nyckel som häver krypteringen och återställer filerna. Utpressningsprogram hör numera till de mest besvärliga cyberhoten mot privatpersoner, företag och andra organisationer. Förlusterna beräknas globalt uppgå till flera hundra miljoner dollar.

Ransomwareangrepp som riktats mot organisationer har tidigare främst förekommit i servicebranschen, industrin och bank- och finansvärlden. Inom social- och hälsovårdssektorn har man under de senaste åren upptäckt utpressningsprogram som riktats bland annat mot sjukhus. Det så kallade WannaCry-programmet (även känt som wCry och WanaCrypt0r) gav upphov till omfattande och allvarliga skador inom flera sektorer i hela världen i maj 2017. I Finland har WannaCry hittats åtminstone i bilddiagnostikdatorer på Åbo universitetscentralsjukhus. Ett angrepp med betydligt värre konsekvenser än de i

Finland inträffade i Storbritannien och riktades mot National Health Service-systemet, där segmenteringen av datanäten hade varit bristfällig och det hade funnits ett stort antal datorer som inte uppdaterats. I Storbritannien tvingades man rentav avvisa patienter vid sjukhusens dörrar.

Skadliga program som används för att bryta virtuell valuta belastar den kapade datorns resurser, vilket leder till att de system i sjukhusmiljön som är viktiga för patientens vård eller socialvårdens klientdata inte fungerar korrekt eller blir långsamma.

Social- och hälsovårdsorganisationer kan utsättas för nätfiske där man försöker komma åt uppgifter genom att skicka e-post till de anställda. Offren kan till exempel få ett e-postmeddelande med rubriken ”Nedladdat dokument”. Meddelandet innehåller en länk till en inloggningssida som liknar Microsoft SharePoint men som dock finns någon helt annanstans. När offret skriver in användarnamnet och lösenordet exempelvis till sitt Office365-konto får svindlarna tag i dem och kan ta kontroll över organisationens e-postkonto. De kapade e-postkontona kan användas till exempel för faktureringsbedrägeri, identitetsstölder och spridning av skadligt material.

Hot och sårbarheter i anslutning till medicinteknisk utrustning

Tillverkarnas fjärråtkomst till olika anordningar kan orsaka sårbarhet. Tillverkarna kan använda fjärråtkomst för att övervaka och reglera medicintekniska produkter, såsom strålbehandlingsapparater, för att lättare förutse fel i utrustningen och åtgärda dem snabbare. Det kräver dock att hälso- och sjukvårdsaktörerna öppnar anslutningar mellan sina interna nätverk och internet, vilket för att genomföras tryggt kräver exakt information om fjärråtkomsttekniken samt noggrannhet i genomförande och övervakning. Tillverkarna kan och vill inte alltid lämna ut detaljer om sin fjärråtkomst. Genom fjärråtkomst förskjuts även den yttre gränsen för hälso- och sjukvårdsproducentens interna nätverk till den yttre gränsen för tillverkarens interna nätverk. Då måste hälso- och sjukvårdsproducenten bland annat genom avtal säkerställa att tillverkarens informationssäkerhet är åtminstone på samma nivå. Det rekommenderas att standardenliga it-processer används för att koppla medicinteknisk utrustning till nätverk (t.ex. ITIL). [4]

Många medicintekniska produkter är försedda med mjukvaruprogram. I programmen upptäcks ofta fel, dvs. sårbarheter, som om de missbrukas kan äventyra en korrekt användning av produkterna. Medicintekniska produkter ska följa tillämpliga standarder och andra officiella krav. Tillverkaren ansvarar för att programmen uppdateras och att de medicintekniska produkterna repareras i övrigt. När man reparerar program i medicintekniska

4 https://tutcris.tut.fi/portal/files/12912971/Jauhiainen_Varri_selvitys_elokuu2017.pdf

produkter ska tillverkaren på nytt säkerställa att programmet uppfyller standarderna. Detta kan leda till att kända sårbarheter i utrustningens program åtgärdas långsamt. Reparationer av använd och lagerhållen utrustning medför ofta extra arbete för både tillverkaren och användarna.

Svårfungerande program kan locka vårdpersonalen till att kringgå de datatekniska skyddsmekanismerna, till exempel så att flera personer använder datasystemet med ett och samma användarnamn eller att standardlösenord inte byts ut.

Hot mot verksamhetsmiljön

Hälso- och sjukvårdens lokaler är öppna vilket försvårar det fysiska skyddet av deras cybermiljö. Det är svårt att upptäcka och avvärja en inkräktare som kommer åt den digitala utrustning och infrastruktur som ska skyddas. Skyddet och hanteringen av hemma- och distansvårdens cybermiljö kan ofta inte kontrolleras av vårdorganisationen.

Det ökade utbudet av social- och hälsovårdstjänster som utförs i hemmet medför nya utmaningar för cybersäkerheten i sektorn. Framtidens cyberhot kan vara bland annat:

- Intrång i medicinteknisk utrustning som kopplats till datanätet, med beaktande särskilt av apparater som används i mycket olika miljöer i vården hemma hos patienterna.
- Kopiering av RFID-chips5 (används t.ex. för passerkontroll).
- Överbelastningsangrepp i molnbaserade system, såsom patient- och klientdatasystemen eller Kanta-tjänsterna.
- Mänskliga misstag i konfigureringen av system eller misstag som görs av vårdpersonalen, med tanke på att den uppkopplade utrustningen ofta kräver specialkompetens både gällande den tekniska användningen och informationssäkerheten.
- Systemstörningar i program och nätuppkopplingsutrustning samt andra nätverkskomponenter.
- Problem med leveranskedjor, t.ex. hos den som tillhandahåller en molntjänst eller tillverkar utrustning.

Beredskap för störningssituationer

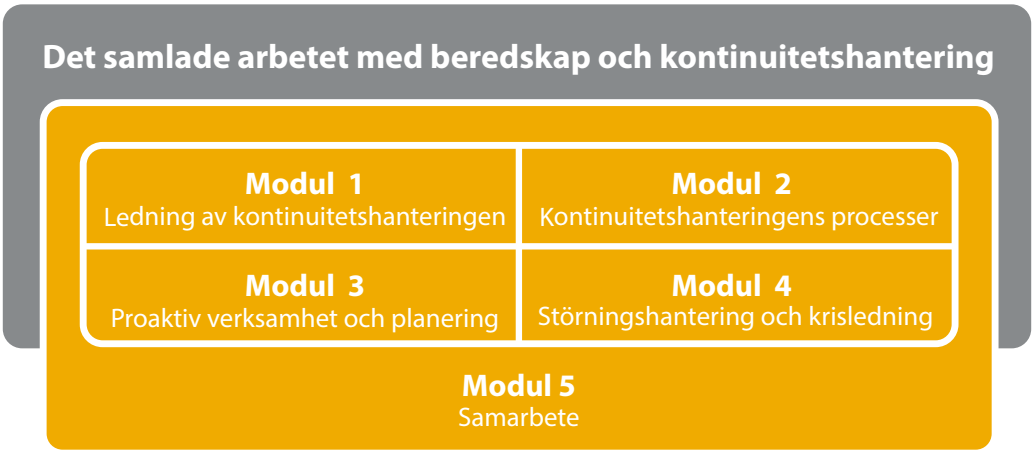
Beredskapen inom social- och hälsovårdstjänsterna grundar sig på högklassig verksamhet under normala förhållanden och förutseende av störningssituationer. Organisationens

5 RFID= (radio frequency identification) fjärridentifieringsmetod med radiofrekvens

förmåga att fungera och producera kritiska tjänster även i störningssituationer förutsätter att ledningen förbinder sig att utveckla beredskapen och verksamhetens kontinuitet samt att personalen engageras och deltar i genomförandet av beredskapen.

Social- och hälsovårdens beredskapsskyldighet grundar sig bland annat på beredskapslagen och de författningar som gäller särskilt för branschen. De organisationer som producerar social- och hälsovårdstjänster ska enligt lagen genom beredskapsplaner förbereda sig på störningssituationer och undantagsförhållanden (t.ex. 12 § i beredskapslagen 1552/2011). I organisationens beredskapsplan antecknas bland annat de olika aktörernas ansvar och roller, hur störningssituationer ska hanteras och ledas samt hur man ska gå till väga för att återhämta sig från en störningssituation.

För social- och hälsovårdsaktörerna utges anvisningar för att stödja beredskapsplaneringen och kontinuitetshanteringen. Anvisningen[6] grundar sig på konceptet för kontinuitetshantering i kommunerna (KUJA) och de relaterade verktygen (bl.a. KUJA-utvärderingsmodellen)[7] som tagits fram av Finlands Kommunförbund. En kontinuitetshanteringshelhet enligt KUJA-modellen beskrivs i figur 2.



Figur 2. Tryggandet av beredskapen och kontinuitetshanteringen (Källa: KUJA-projektet, Finlands Kommunförbund)

En central beredskapsåtgärd är att definiera kritiska funktioner, tjänster och system, såsom utrustning och program. Dessa ska säkerställas i alla situationer. Dessutom ska man

6 Planering av beredskap och kontinuitetshantering. Anvisning för aktörer inom social- och hälsovården. Social- och hälsovårdsministeriet 2019 (2019:16)

7 KUJA-konceptet och verktygen: www.kuntaliitto.fi/kuja

identifiera de kritiska stödtjänster och funktioner som behövs för att sköta de kritiska uppgifterna.

Ledningen av störningssituationer grundar sig på organisationens dagliga ledning. Organisationens ledning ska sörja för och säkerställa exempelvis en tillräcklig resursfördelning för samt uppföljning och styrning av beredskapen. Kontinuitetshantering och beredskap, liksom även informationssäkerhet, ska vara en permanent del av organisationens övriga verksamhet, processer och tjänster.

Det gäller att ha beredskap för långvariga störningar i informationssystem samt att planera och öva sätt för att klara av dem. Vid behov ska organisationerna kunna fungera utan informationssystem under undantagsförhållanden. Tillförlitligheten hos de informationssystem som klassificerats som de mest kritiska ska säkerställas med hjälp av exempelvis fungerande säkerhetskopiering, planerade tillfälliga lösningar, reservdelar, specialkomponenter samt aktiva övervaknings- och underhållsåtgärder[8].

Riskhantering

Riskhantering är en metod för att säkerställa organisationens funktion i störningssituationer. Det finns olika verktyg för riskanalyser och riskhantering.

Med hjälp av riskhantering identifieras de kritiska riskerna. Det gäller att identifiera tjänsternas och systemens betydelse för organisationens verksamhet och bedöma hotens (inklusive informationssäkerhets- och cybersäkerhetshoten) inverkan på tjänsternas och systemens funktionsförmåga. Riskbedömning ska inkluderas i organisationens planerade verksamhet enligt årsklockan. Utöver att ledningen ska vara medveten om eventuella risker ska den också bedöma och godkänna de åtgärder som planerats för att minska riskerna och följa upp genomförandet av dem.

Organisationen ska ha klara verksamhetsprinciper för sina säkerhetsutredningsförfaranden. Organisationen har skyldighet att sörja för klassificeringen av information (egen information eller information som tillhör en annan myndighet) och en ändamålsenlig behandling av information bland annat genom att säkerställa att den person som har rätt till informationen är tillförlitlig.[9] Detta ska bevisas genom en säkerhetsutredning av personen i fråga. Säkerhetsutredningsförfarandet i organisationerna ska omfatta de personer i tjänste- och anställningsförhållande som kan ha tillgång till information och/eller lokaler som ska skyddas.

8 VAHTI-anvisningen 2/2016 http://urn.fi/URN:ISBN:978-952-251-779-1

9 Säkerhetsutredningslagen 726/2014, riksdagen godkände RP 284/2018 som ny lag om informationshantering 19.3.2019. Lagen innehåller även bestämmelser om klassificering av information.

Ett exempel på ett verktyg för riskhantering är VAHTI-anvisningen, som beskriver hur ISO31000-standarden ska tillämpas.[10] Standarderna bildar en referensram och stomme för den långsiktiga utvecklingen av verksamheten. I bilaga 5 presenteras standarder och referensramar som är viktiga för hälso- och sjukvården. I Finland är kända standarder ISO/IEC 27000 (informationssäkerhet), 9000 (kvalitet) samt 30000 (riskhantering). Bilaga 5 innehåller också en förteckning över auditeringsverktyg och certifieringsmodeller.

Upphandling och avtal

Avtalsbaserad beredskap är en viktig del av den övergripande beredskapen. Den egna verksamhetens kontinuitet och en störningsfri service ska säkerställas även i fråga om utlagda tjänster, såsom stödtjänster och materialleveranser. Informationssäkerhet, dataskydd och kontinuitetshantering ska inkluderas bland annat i serviceavtalen.

Informationssäkerhets- och dataskyddsriskerna ska beaktas redan i det skede då kriterier fastställs och upphandlingen utförs. Dessa ska med fördel beaktas redan i avtalsvillkoren. I informationssäkerhetskraven för upphandlingar ska upphandlingsobjektets hela livscykel beaktas allt från själva upphandlingen till användningen och avskaffandet av objektet. Skyddet för informationshanteringsmiljön och dess ändamålsenliga funktion ska säkerställas under hela livscykeln (underhåll, hantering och övervakning). Annars kan det hända att den utrustning eller det informationssystem som upphandlas ur informationssäkerhetsperspektiv föråldras snabbt efter ibruktagandet.

Inom Försörjningsberedskapscentralens cybersäkerhetsprojekt utvecklas en databas för informationssäkerhetskrav som grundar sig på de vanligaste informationssäkerhetsstandarderna (t.ex. ISO27001). Det är möjligt att delvis tillämpa samma kriterier på sjukhusutrustning och industriell automatik eftersom bägge grundar sig på automatiska system. Utvecklingsbehov har identifierats i synnerhet i fråga om den medicintekniska utrustningens informationssäkerhetskrav.

I de kommande VAHTI100-anvisningarna klargörs punkterna om informationssäkerhet i lagen om informationshantering i närmare detalj. I den tidigare motsvarande anvisningen beskrivs kraven på den tekniska datateknikmiljön och verktygen för konkurrensutsättning och upphandling.[11]

Att beakta informationssäkerhetskraven i upphandlingar innebär i praktiken ofta att utveckla upphandlingsprocesserna. För att informationssäkerhetskraven ska kunna anpassas korrekt till varje upphandling måste man inom organisationen bedöma

10 VAHTI, Riskhanteringsanvisning, Finansministeriets publikationer 22/2017 http://urn.fi/URN:ISBN:978-952-251-862-0

11 Vahti 3/2012 Teknisen ympäristön tietoturvataso-ohje, https://www.vahtiohje.fi/web/guest/3/2012-teknisen-ymparistontietoturvataso-ohje. Vahti100-anvisningarna är under beredning.

upphandlingskraven i ett tillräckligt tidigt skede. Detta innebär att beakta alla nödvändiga parter i de olika skedena av upphandlingsprocessen, bland annat att gå igenom upphandlingskraven med dem som ansvarar för den medicinska tekniken, informationsförvaltningen och dataskyddet. Kraven ska säkerställas i upphandlingar och avtal.

Utbildning och övning

Målet med utbildningen är att varje anställd ska känna till organisationens informationssäkerhets- och dataskyddsprinciper och kunna tillämpa dem i sitt arbete. Informationssäkerhets- och dataskyddskompetensen ingår i upprätthållandet av yrkeskunskapen och fortbildningen. Introduktionen i informationssäkerheten och dataskyddet börjar redan när anställningen inleds och fortsätter genom hela karriären. Organisationerna ska se till att de anställdas informationssäkerhets- och dataskyddskompetens kartläggs och aktivt uppmuntra till fortbildning.

Som en del av utbildningen ordnas övningar utifrån risker, hotbedömningar, sårbarheter och identifierade utvecklingsobjekt. I övningarna ska även sådana aktörer delta som har en central roll i verkliga störningssituationer. På så sätt kan man säkerställa att övningsresultaten effektivt förankras i den praktiska verksamheten.

Cyberstörningssituationer kan vara en del av ett mer omfattande försök att påverka samhällets funktioner (hybridpåverkan). Därför är det mycket viktigt att i störningssituationer planenligt förmedla en lägesbild till samarbetspartner och ett nätverk utöver den egna organisationen.

Hanteringsmodell för störningssituationer

I figur 3 presenteras en hanteringsmodell för cyberstörningssituationer på allmän nivå med beaktande av verksamheten på det lokala och regionala planet samt inom statsförvaltningen. Modellen grundar sig på en modell för de fem specialansvarsområdena inom hälso- och sjukvården som har visat sig vara effektiv bland annat inom Försörjningsberedskapscentralens projekt för cyberhälsa. Det är fråga om en allmän beskrivning som inte i detalj redogör för organisationernas strukturer och ansvar. För att man vid störningar som sträcker sig ovanför lokalnivå ska kunna skapa en lägesbild och stödja aktörerna effektivt ska information samlas in och förmedlas på ett tillräckligt stort verksamhetsområde. Bland annat i Försörjningsberedskapscentralens projekt har modellen för de fem specialansvarsområdena blivit en naturlig struktur för hälso- och sjukvården. På statsrådsnivå är bland annat Cybersäkerhetscentret en väsentlig aktör i cyberstörningssituationer. Ministerierna tar fram en lägesbild för statsrådets lägescentral. Modellen för störningssituationer ska vidareutvecklas och testas genom övningar.

Identifiering av störningssituationer och reaktionsförmåga

Hanteringen av en cybersäkerhetsstörning börjar när någon upptäcker en incident i cybermiljön. De inledande skedena av hanteringen är ofta samma oberoende av organisationens grundläggande uppgift och roll. En incident kan vara t.ex.

- en störning i IKT-tjänsterna
- en situation som äventyrar IKT-tjänsternas funktion, såsom ett elavbrott
- röjande av sekretessbelagd information i digital form för utomstående

Det centrala är att bedöma störningens typ och det eventuella hotet mot organisationens verksamhet, patient- och klientsäkerheten, dataskyddet och integritetsskyddet. Störningen kan hänföra sig exempelvis till patientdatasystemet, den medicintekniska utrustningens funktion eller överföringen av uppgifter. Utifrån bedömningen ska man besluta om störningen förutsätter omedelbara åtgärder.

I diagrammet för hanteringsmodellen för störningssituationer fungerar en social- och hälsovårdsproducent som mottagare av störningsanmälan, men verksamheten följer samma mönster även i andra organisationer som upptäcker eller misstänker cyberstörningar.[12]

Informationssystemets administratör ska omedelbart få information om en misstänkt eller upptäckt störning. Vid cyberstörningar i kontorsmiljö tas störningsanmälningar vanligen emot av informationsförvaltningens helpdesk. Om störningen gäller medicintekniska produkter kan den anmälas till den ansvariga person som organisationen uppgett. Det kan också löna sig att omedelbart rapportera om störningen till tillverkarna av fjärrstyrda medicintekniska produkter, såsom bilddiagnostiska apparater.

Störningen kan upptäckas av personalen i den organisation som äger informationssystemet eller av en kund, avtalspart eller en utomstående. Informationssystemets ägare och administratör ska ha tillgång till flera olika kanaler för att hantera störningsanmälningar. Även informationssystemens användare ska veta vem de ska meddela om störningar. Informationsförvaltningens eventuella helpdesk ska gärna ha tillgång till information om vem som ansvarar för olika system.

12 Den process för hantering av störningar som beskrivs i delen om social- och hälsovårdsproducenter i diagrammet motsvarar processen för hantering av informationssäkerhetsincidenter i VAHTI-anvisningen (Finansministeriets publikationer 8/2017, s. 15 figur 2 Tietoturvapoikkeamien käsittelyprosessi). Med termen informationssäkerhetsincident i VAHTI-anvisningen avses samma fenomen som cyberstörning i denna anvisning. http://urn.fi/URN:ISBN:%20978-952-251-930-6

När en störning börjar finns det oftast inte information om huruvida störningen har uppstått av misstag eller avsiktligen. Det finns dock vissa betydande skillnader mellan att hantera en avsiktlig och en oavsiktlig störning. Därför ska situationen regelbundet bedömas på nytt i takt med att lägesbilden klarnar, och den eventuella cyberangriparen ska inte ges fördel genom oöverlagda åtgärder för störningshantering.

Ägaren av informationssystemet bedömer situationen och gör vid behov en störningsanmälan ("Preliminär analys" -> "Är det en cyberstörning?"). Om personalen hos informationssystemets ägare inte har kapacitet att bedöma cyberstörningen ska den komma överens om bedömningen till exempel med den IKT-tjänsteleverantör som administrerar systemet.

Den första störningsanmälan är sällan så detaljerad att det är möjligt att skapa en tillförlitlig lägesbild enbart utifrån den. Man bör utan dröjsmål be om mer information av den som anmält störningen. Om man på ett tillförlitligt sätt kan utesluta möjligheten av en cyberstörning ska situationen hanteras som en normal stödbegäran (”Hantering enligt stödtjänstprocesserna”).

Hantering av cyberstörningssituationer

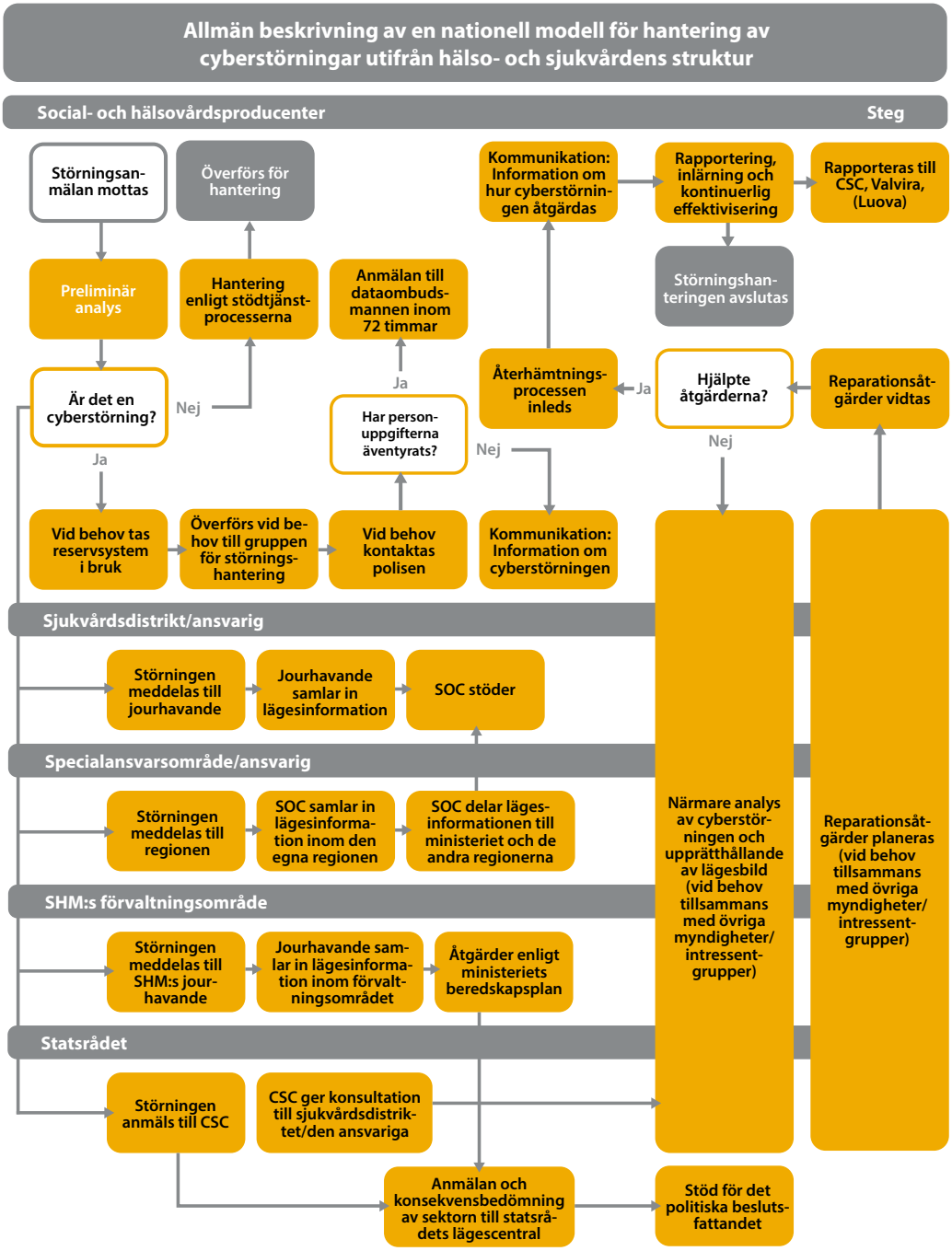
Om man utifrån en första bedömning misstänker att det är fråga om en cyberstörning ska informationssystemets ägare inleda ett flertal åtgärder. För det första ska man begränsa skadorna och inleda en preliminär återhämtning. I vissa situationer kan det innebära att man tar ett reservsystem i bruk (”Vid behov tas reservsystem i bruk”). Ofta är det inte möjligt att utifrån de preliminära uppgifterna om situationen bedöma om patienternas vård och klienternas service orsakas mer skada av att man exempelvis övergår till ett reservsystem än av att man fortsätter använda det system som är utsatt för störningen. Man bör på nytt överväga om reservsystemet ska tas i bruk när lägesbilden klarnar. Det gäller också att beakta den eventuella inverkan på Kanta-tjänsterna och skyldigheten att göra en anmälan till Kanta-tjänsterna.

För det andra ska systemets ägare höja beredskapen för att hantera störningssituationen. Ägaren ska överväga att överföra hanteringen av störningen till en grupp som har erfarenhet av att hantera cyberstörningar och som kan bestå av ägarens egen personal eller av personer som har anlitats via en avtalspartner (”Överförs vid behov till gruppen för störningshantering”).

Vid misstanke om brott ska man fort kontakta polisen (”Vid behov kontaktas polisen”). Polisen kan för att förebygga och utreda brott använda tvångsmedel och informationskällor som andra myndigheter inte har tillgång till. Informationssystemets ägare ska på förhand utforma en anvisning om vem som får göra en brottsanmälan i ägarens namn och

hur det säkerställs att dessa personer är tillgängliga även under lediga dagar och semestrar. I allmänhet lönar det sig att ålägga samma personer ansvaret för beslutsfattandet i brådskande ärenden som gäller produktionen av IKT-tjänster.

I figur 3 finns en allmän beskrivning av en nationell modell för hantering av cyberstörningar som grundar sig på hälso- och sjukvårdens struktur.



Figur 3. Allmän beskrivning av en nationell modell för hantering av cyberstörningar utifrån hälso- och sjukvårdens struktur.

Anmälan om cyberstörningar till tillsynsmyndigheterna

När cyberstörningen är över ska social- och hälsovårdsorganisationen vara beredd att ge en detaljerad förklaring om störningssituationens inverkan på patientsäkerheten till regionförvaltningsverket. Yrkespersoner inom social- och hälsovården har skyldighet att anmäla farliga situationer som orsakas av produkter och utrustning för hälso- och sjukvård även till den övervakande myndigheten (Valvira). Till efterarbetet vid hanteringen av betydande cyberstörningar hör dessutom en anmälan till Valvira enligt EU:s direktiv om nät- och informationssäkerhet (det s.k. NIS-direktivet).

Det är bra att göra en frivillig anmälan om störningen till Cybersäkerhetscentret vid Traficom (”Störningen anmäls till CSC ” i figur 3), som kan ge råd och stöd för hanteringen av incidenten (”CSC ger konsultation till sjukvårdsdistriktet/den ansvariga” i figur 3). Cybersäkerhetscentret upprätthåller en nationell lägesbild av cybersäkerheten.

Informationssystemets ägare ska alltid i samband med en störning bedöma om dataskyddet äventyrats i (”Har personuppgifterna äventyrats?”). Vid en personuppgiftsincident ska den personuppgiftsansvarige utan onödigt dröjsmål och, om så är möjligt, inte senare än 72 timmar efter att ha fått vetskap om den, anmäla personuppgiftsincidenten till dataombudsmannens byrå, såvida det inte är osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter. Om anmälan till tillsynsmyndigheten inte görs inom 72 timmar ska den åtföljas av en motivering till förseningen.

Information om cyberstörningar

Oavsett om skyddet för personuppgifter äventyrats ska informationssystemets ägare informera dem som berörs av störningen om incidenten (”Kommunikation: Information om cyberstörningen”). De allmänna kriskommunikationsanvisningarna lämpar sig även för att informera om cyberstörningar.

Informationssystemets ägare ska överväga om situationen är så allvarlig att även de högre nivåerna inom den offentliga förvaltningen eller de centrala samarbetsorganisationerna ska informeras. Det är bra att diskutera med intressentgrupperna om vad som ska anmälas och vilken information som ska delas redan innan en störning inträffat.

I princip är det bättre att informera om en störning än att låta bli. Organisationer som tillhandahåller offentliga social- och hälsovårdstjänster ska anmäla cyberstörningar som gäller den egna verksamheten till beställarna av organisationens tjänster. De högre förvaltningsnivåerna är framför allt intresserade av orsaken till störningen, återhämtningsplanen och den anmälande organisationens förmåga att klara av sina normala uppgifter. Samarbetsorganisationerna är vanligen mer intresserade av störningens tekniska detaljer så att de kan bedöma om det egna skyddet är tillräckligt.

En närmare analys av informationssäkerhetsincidenterna ska inledas genast när tillräckligt många personer kan undvaras från de nödvändiga preliminära åtgärderna (”Närmare analys av cyberstörningen och upprätthållande av lägesbild”). För att kunna göra en noggrann analys krävs kontrollerade fakta om vad som hänt och när samt vem eller vad som ligger bakom händelsen. I allmänhet är logguppgifter i datorer och IKT-tjänster oersättliga. Även leverantörerna av fjärrstyrda medicintekniska produkter kan ha viktiga metriska data som behövs för att förstå och reda ut störningen.

En analys förutsätter dock i allmänhet samarbete med intressentgrupperna, exempelvis leverantörerna av IKT-tjänster. Det är bra att komma överens om samarbetet i god tid: vem har rätt att be om hjälp mot en eventuell avgift, vilka uppgifter får delas med vilka redskap osv.

Utifrån den analyserade lägesinformationen ska informationssystemets ägare tillsammans med sina intressentgrupper planera vad som behöver göras för att åtgärda störningen (”Reparationsåtgärder planeras”). I synnerhet om det ligger en målmedveten angripare bakom störningen ska reparationsåtgärderna (inklusive informationen) planeras så att angriparen kan hejdas med en gång. Reparationsåtgärderna inkluderar även att bevismaterial och händelseloggar sparas för senare bruk. Polisen och Cybersäkerhetscentret kan ge råd om hur man sparar ned digitalt bevismaterial.

Även de anställda som deltar i systemunderhållet och som påverkas av reparationsåtgärderna ska informeras om dessa. Meddelandet kan formuleras enkelt: ”Vi vidtar nu följande åtgärd och meddelar om en timme hur vi går vidare.”

Informationssystemets ägare och dess intressentgrupper ska genomföra reparationsåtgärderna på ett planerat och koordinerat sätt (”Reparationsåtgärder vidtas”). Reparationsåtgärdernas effekt ska följas upp (”Hjälpte åtgärderna?”). Om åtgärderna inte har tillräcklig effekt ska analyseringen och åtgärdandet av cyberstörningen fortsätta.

Återhämtning från cyberstörningar och lärdom

När informationssystemets ägare har fått kontroll över en akut störningssituation ska återhämtningsprocessen inledas så att man kan återgå till den normala verksamheten (”Återhämtningsprocessen inleds”). Även den ska planeras och förberedas på förhand. Om man exempelvis under incidenten har tagit ett reservsystem i bruk ska de uppgifter som registrerats i detta överföras till det egentliga systemet som en del av återhämtningen. Att informera intressentgrupperna om att den avvikande situationen upphört hör till återhämtningen (”Kommunikation: Information om hur cyberstörningen åtgärdas").

Att snabbt och säkert få kontakt med den jourhavande personalen är en viktig del av hälso- och sjukvårdsproduktionen. De allmänna kommunikationstjänsterna kan ibland utsättas för funktionsstörningar som varar i flera timmar. Tjänsteleverantören ska uppskatta hur länge den kan fungera utan tillgång till de allmänna kommunikationstjänsterna och med vilka metoder den kan förbereda sig för störningar i dessa. Vanliga beredskapsmetoder är

- reservabonnemang från flera olika teleföretag
- användning av myndigheternas radionät (VIRVE) vid sidan om mobiltelefonabonnemang
- interna högtalar- och informationssystem i sjukhus

När störningssituationen upphört ska man ordna ett möte för att tillsammans gå igenom situationen och dess inverkan på verksamheten samt de brister som uppdagats. Man utvärderar hur bra situationen hanterats tillsammans med de anställda och intressentgrupper som varit involverade i störningssituationen. Väsentliga uppgifter om farliga situationer och störningar ska samlas in och erfarenheter och slutledningar delas om hur säkerheten och verksamheten kan förbättras till nytta för alla aktörer. Dessutom ska man slå fast hur brister ska åtgärdas och hur detta följs upp. Samtidigt kontrolleras och justeras befintliga anvisningar och planer.

Störningssituationer är värdefulla tillfällen att ta lärdom av och förbättra verksamheten (”Rapportering, inlärning och kontinuerlig effektivisering”). Hanteringen av en incident kan inte anses ha slutförts effektivt innan man har identifierat på vilka punkter man lyckats bra, vilka brister som finns och hur verksamheten kan förbättras. I återhämtnings-, lärdoms- och utvecklingsprocessen ingår en plan för egenkontroll av dataskyddet och informationssäkerheten och dokumentering av de egna övervaknings- och beredskapsåtgärderna. Lärdomarna av störningssituationer ska med fördel rapporteras till Cybersäkerhetscentret, som ger respons och som med rapportörens tillstånd anonymt kan sprida lärdomarna till andra.

Sjukvårdsdistriktens roll i cyberstörningssituationer

Sjukvårdsdistriktet ska ha kapacitet att ta emot och hantera anmälningar om cyberstörningar som gäller de egna informationssystemen och verksamheten i de organisationer som producerar avtalsbaserade social- och hälsovårdstjänster.

Sjukvårdsdistriktet ska bedöma vilken effekt cyberstörningen har på dess förmåga att sköta sina uppgifter. Cyberstörningar ska rapporteras vidare för att skapa en mer omfattande lägesbild på det regionala och nationella planet. Ofta drabbar cyberstörningar samtidigt flera organisationer som kanske inte finns i samma sjukvårdsdistrikt eller ens

i samma specialupptagningområde. I den modell för hantering av cyberstörningar som presenterats ovan ska en anmälan göras till övriga centrala myndigheter enligt modellen. Specialupptagningområdena[13] ska ha kapacitet att ta emot och bedöma anmälningar om cyberstörningar inom sitt eget verksamhetsområde och skapa en nationell lägesbild tillsammans med de övriga områdena och Cybersäkerhetscentret.

Social- och hälsovårdsministeriets och dess inrättningars roll i cyberstörningssituationer

De inrättningar som lyder under social- och hälsovårdsministeriet upprätthåller kapaciteten att observera och reagera på cyberhot på samma sätt som i branschen i övrigt. Inrättningarna rapporterar om betydande störningar till social- och hälsovårdsministeriet och Cybersäkerhetscentret. Valvira mottar även anmälningar om cyberstörningar som gäller patientdatasystem som kan jämställas med medicinteknisk utrustning eller delar av dessa.

Social- och hälsovårdsministeriets beredskapsenhet upprätthåller situationsledningsberedskapen för störningssituationer i förvaltningsområdet samt ministeriets kontinuerliga joursystem. I avvikande situationer leds social- och hälsovårdsministeriets verksamhet till en början av den som har beredskapsjour och därefter av den tjänsteman som ansvarar för verksamheten, beredskapschefen eller ministeriets ledning. I exceptionella situationer har ministeriets beredskapsorganisation i uppgift att upprätthålla en nationell lägesbild i synnerhet genom att se till att social- och hälsovårdsministeriet och statsrådets lägescentral har en gemensam lägesbild. Dessutom ska social- och hälsovårdsministeriets beredskapsorganisation efter behov hålla kontakt med de jourhavande vid de andra ministerierna, Valvira, Cybersäkerhetscentret och aktörerna i branschen. Social- och hälsovårdsministeriet ska informera statsrådets lägescentral om betydande störningar inom sitt förvaltnings- och verksamhetsområde.

Cybersäkerhetscentrets och statsrådets lägescentrals roll vid cyberstörningar

Cybersäkerhetscentret tar emot anmälningar om säkerhetsöverträdelser från alla aktörer. I egenskap av försörjningsberedskapskritiska organisationer får sjukvårdsdistrikten privilegierad service. Övriga anmälare betjänas så fort situationen tillåter det.

Sjukvårdsdistrikten kan via Cybersäkerhetscentrets blankett på webben göra en anmälan om betydande säkerhetsincidenter till Valvira i enlighet med EU:s direktiv om nät- och informationssäkerhet (NIS-direktivet). Sjukvårdsdistriktet kan om det så önskar delge

13 Vissa specialsjukvårdstjänster ordnas över sjukvårdsdistriktens gränser utifrån universitetssjukhusens specialupptagningområden, dvs. de så kallade miljondistrikten. I statsrådets förordning 156/2017 anges vilka specialupptagningsområden är och vilka sjukvårdsdistrikt som hör till vilket område.

Cybersäkerhetscentret samma anmälan. Cybersäkerhetscentret förmedlar i princip inte uppgifter som det fått till andra på ett sådant sätt att dessa kan identifiera anmälaren eller föremålet för cyberstörningen. Centret rapporterar uppgifterna till andra endast med anmälarens tillstånd eller om störningen äventyrar människornas hälsa eller liv eller samhällets säkerhet.

Cybersäkerhetscentret ger råd om vilka första åtgärder anmälaren ska vidta för att få kontroll över cyberstörningen. Med hjälp av de uppgifter som Cybersäkerhetscentret mottar upprätthåller centret en nationell lägesbild av cybersäkerheten. Centret koordinerar samarbetet mellan de olika organisationer som behövs för att hantera störningen genom att säkerställa att informationen om störningen analyseras och delas mellan aktörerna.

Cybersäkerhetscentret har inte behörighet att hantera störningar i fråga om andra än de teleföretag som tillhandahåller allmänna kommunikationstjänster. De aktörer som deltar i hanteringen av störningen handlar inom ramen för sina egna befogenheter.

Cybersäkerhetscentret förmedlar information om cyberincidenter som avsevärt stör samhällets funktioner till statsrådets lägescentral, som använder informationen för att komplettera sin egen lägesbild och vid behov informera statsrådet. Det är viktigt att informationen löper via bägge kanalerna för att kontinuitetsaspekterna i fråga om både social- och hälsovårdsproduktionen och de digitala systemen ska kunna beaktas.

Upprätthållande och utveckling av anvisningen

Cybersäkerheten ska upprätthållas kontinuerligt och processen utvecklas eftersom även hoten ändrar form. Denna anvisning ska hanteras och uppdateras som en fortlöpande process. En första version av anvisningen publiceras i social- och hälsovårdsministeriets publikationsserie. Social- och hälsovårdsaktörerna deltar i uppdateringen av anvisningen.

Källförteckning

Iyengar, A., Kundu, A., & Pallis, G. (2018). Healthcare Informatics and Privacy. IEEE Internet Computing, 22(2), 29–31.

Nationell riskbedömning 2018, Inre säkerhet. Inrikesministeriets publikationer 2019:5. http://urn.fi/URN:ISBN:978-952-324-245-6

Kodin kyberopas – ohjeita digitaaliseen arkeen 2017, Säkerhetskommittén. https://turvallisuuskomitea.fi/kodin-kyberopas-ohjeita-digitaaliseen-arkeen/

Kyber-terveys, nyhetsbrev 3/2018. 5.10.2018 – Hankintojen tietoturva. Försörjningsberedskapscentralen

Cybersäkerhetscentrets internetsidor, Varning 3/2018 (uppdaterats 7.1.2019). Nätfiske och dataintrång mot Office 365-e-postkonton mycket vanliga – upptäck, skydda dig och informera! https://www.kyberturvallisuuskeskus.fi/sv/natfiske-och-dataintrang-mot-office-365-e-postkonton-mycket-vanliga-upptack-skydda-dig-och

Miikael och Martti Lehto 2017 (Jyväskylä universitet) Kyberturvallisuus sairaalajärjestelmissä, Osa 1. https://www.jyu.fi/it/fi/tutkimus/julkaisut/tekes-raportteja/kyberturvallisuus-sairaalassa_-14-8-17.pdf

Lääkärilehtis webbpublikation (8.6.2017). WannaCry-haittaohjelma löytyi TYKS:sta. https://www.laakarilehti.fi/ajassa/ajankohtaista/wannacry-haittaohjelma-loytyi-tyks-sta/

Olycksutredningscentralen; Y2018-02 Datastörningarna i Helsingfors och Nylands sjukvårdsdistrikt 7–8.11.2017. https://turvallisuustutkinta.fi/material/attachments/otkes/tutkintaselostukset/OZnac1oRj/Y2018-02_HUS.pdf

Polisens, CERT-FI:s och F-Secure Pyj:s gemensamma webbplats om beredskap för nätbrottslighet http://www.ransomware.fi/

Smart Hospitals – Security and Resilience for Smart Health Service and Infrastructures (2016). Publikation om cyberhot på smarta sjukhus av EU:s nätverks- och informationssäkerhetsbyrå (ENISA) https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals/at_download/fullReport

Avtalsbaserad beredskap. Anvisning för aktörer inom social- och hälsovården. Social- och hälsovårdsministeriets publikationer 2019:15.

Projektet för verkställande av riksomfattande informationssystemtjänster och strukturerad dokumentation inom socialvården (Kansa-projektet). Projektplan 2016–2020. Institutet för hälsa och välfärd (THL). Styrning 10/2016. http://www.julkari.fi/bitstream/handle/10024/130563/URN_ISBN_978-952-302-660-5.pdf

Riktlinjer för it-förvaltningen inom social- och hälsovårdsministeriets förvaltningsområde 2018–2022, Social- och hälsovårdsministeriets publikationer 11/2018 (på finska). http://urn.fi/URN:ISBN:978-952-00-3949-3

Cybersäkerheten i Finland – nuläge, måltillstånd och nödvändiga åtgärder för att uppnå måltillståndet 2/2017, Publikationsserie för statsrådets utrednings- och forskningsverksamhet 30/2017 (på finska). https://tietokayttoon.fi/julkaisu?pubid=17805

Verkställighetsprogrammet för strategin för cybersäkerhet i Finland 2011–2017. Säkerhetskommittén. (På finska). https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/Toimeenpano-ohjelma-2017-2020-final.pdf

Terveydenhuoltoalan kyberuhkia (2016). Anvisning 1/2016 Kommunikationsverket, Cybersäkerhetscentralen. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Terveydenhuoltoalan_kyberuhkia.pdf

Tammerfors tekniska universitets undersökning om att utnyttja standardenliga it-processer för att koppla upp medicinteknisk utrustning (på finska) https://tutcris.tut.fi/portal/files/12912971/Jauhiainen_Varri_selvitys_elokuu2017.pdf

Planering av beredskap och kontinuitetshantering. Anvisning för aktörer inom social- och hälsovården. Social- och hälsovårdsministeriets publikationer 2019:16.

Finansministeriets publikationer 8/2017, Hantering av informationssäkerhetsincidenter (på finska) http://urn.fi/URN:ISBN:%20978-952-251-930-6

Finansministeriets publikationer 22/2017, Riskhanteringsanvisning (på finska) http://urn.fi/URN:ISBN:978-952-251-862-0

Finansministeriets publikationer 2/2016, Hantering av kontinuiteten i verksamheten (på finska) http://urn.fi/URN:ISBN:978-952-251-779-1

Finansministeriets publikationer 2/2012, ICT-varautumisen vaatimukset https://www.vahtiohje.fi/web/guest/2/2012-ict-varautumisen-vaatimukset

Finansministeriets publikationer 2c/2010, Anvisning om verkställighet av förordningen om informationssäkerheten inom statsförvaltningen https://www.vahtiohje.fi/c/document_library/get_file?uuid=0d24cfd9-19ec-498c-82f1-023c35484cb4&groupId=10229

Transport- och kommunikationsverkets webbplats, Informationssäkerhet nu! (16.2.2018). WannaMine använder gamla tricks – ingen särskild anledning till oro https://legacy.viestintavirasto.fi/sv/cybersakerhet/informationssakerhetnu/2018/02/ttn201802161123.html

Transport- och kommunikationsverket Traficom, Cybersäkerhetscentret. Tietoturvan vuosi 2018. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Tietoturvan_vuosi_%2018_aukeamat.pdf

Vesihuoltolaitosten kyberturvallisuuteen uusia työkaluja kybervesi-hankkeesta, meddelande Försörjningsberedskapscentralen 29.11.2018. https://www.huoltovarmuuskeskus.fi/vesihuoltolaitosten-kyberturvallisuuteen-uusia-tyokaluja-kyber-vesi-hankkeesta/

Von Solms, R., & Van Niekerk, J. (2013) From information security to cyber security Article in Computers & Security 38: 97–102.

Säkerhetsstrategi för samhället 2017, Statsrådets principbeslut/2.11.2017. https://turvallisuuskomitea.fi/wp-content/uploads/2018/04/YTS_2017_svenska.pdf

Bilagor

BILAGA 1

Beskrivning av centrala nationella aktörer

Befolkningsregistercentralen

Befolkningsregistercentralen är ett statligt ämbetsverk som verkar som operativ aktör för ledningsgruppen för informations- och cybersäkerheten inom statsförvaltningen (VAHTI), som tillsatts av finansministeriet. Befolkningsregistercentralen utvecklar i samarbete med Cybersäkerhetscentret vid Transport- och kommunikationsverket informations- och cybersäkerhetstjänster för den offentliga förvaltningen. Befolkningsregistercentralen producerar även avgiftsbelagda sakkunnigtjänster inom digital säkerhet för kunder inom den offentliga förvaltningen.

Cybersäkerhetscentret (CSC)

Cybersäkerhetscentret vid Traficom har till uppgift att övervaka hot mot cybersäkerheten och sammanställa information om cybersäkerhet för olika aktörer. Centret varnar för större cyberhot och riktar även upplysning till medborgarna. Cybersäkerhetscentret verkar både inom den offentliga och privata sektorn. Centret tillhandahåller effektiviserade tjänster för försörjningsberedskapskritiska organisationer, däribland många organisationer inom social- och hälsovården:

- förtur inom CERT-tjänster,
- informationsutbyte inom social- och hälsovårdssektorn och lägesbedömningar av aktuella cyberhot,
- konfidentiell grupp för utbyte av information inom social- och hälsovården (SOTE-ISAC), vars medlemsorganisationer utbyter information om säkerhetsincidenter och sprider god praxis till andra i branschen,
- rådgivningstjänst för hur organisationerna kan utveckla cybersäkerheten samt möjlighet att anlita en tjänst som upptäcker och varnar för allvarliga säkerhetsöverträdelser (HAVARO). Tjänsten är avsedd att komplettera kundorganisationernas övriga informationssäkerhetskontroller.

Genom rådgivningstjänsten hjälper Cybersäkerhetscentret de försörjningsberedskapskritiska organisationerna att bedöma utvecklingsbehoven i cybersäkerheten. Cybersäkerhetscentret bedriver även internationellt samarbete inom ramen för cybersäkerheten inom hälso- och sjukvården. Centret representerar Finland i det inofficiella samarbetet

Health CERTs som är avsett för cybersäkerhetsaktörer inom hälso- och sjukvården. Inom gemenskapen byter man information om aktuella cyberhot inom hälso- och sjukvården och om hur cybersäkerheten i sektorn kan utvecklas.

Privatpersoner, företag och organisationer kan till Cybersäkerhetscentret anmäla säkerhetsöverträdelser som de utsatts för, såsom nätfiske och överbelastningsangrepp samt försök till dessa. Cybersäkerhetscentret gör en bedömning av allvarlighetsgraden utifrån vilken man vid behov vidtar extra åtgärder för att reda ut situationen.

Finansministeriet (FM)

Finansministeriet svarar för styrningen och utvecklingen av statens informationssäkerhet.

Verksamheten grundar sig på varje organisations ansvar för informationssäkerheten i sin egen verksamhet, de skyldigheter om informationssäkerhet som fastställs i lag, statsrådets principbeslut om utvecklingen av statens informationssäkerhet, cybersäkerhetsstrategin i Finland och finansministeriets informationssäkerhetsanvisningar (VAHTI) och övriga riktlinjer.

Folkpensionsanstalten (FPA)

FPA ansvarar för uppbyggnaden, testningen och underhållet av Kanta-tjänsterna. FPA ansvarar också för de tekniska specifikationerna i samband med anslutning till Kanta-tjänsterna samt för säkerställandet av anslutningsförutsättningarna. FPA är även registeransvarig för det nationella Receptcentret och sköter det datatekniska underhållet av Receptcentret.

För att informationssystem ska kunna anslutas till Kanta-tjänsterna krävs certifiering, vilket innebär att de väsentliga kraven ska tillämpas på informationssystemen enligt Institutet för hälsa och välfärds föreskrifter. Dessutom ska systemen testas tillsammans med Kanta-tjänsterna, informationssäkerheten bedömas av ett så kallat godkänt bedömningsorgan för informationssäkerhet samt resultatens överensstämmelse med kraven bevisas.

Försörjningsberedskapscentralen (FBC)

Försörjningsberedskapscentralen är en inrättning inom arbets- och näringsministeriets förvaltningsområde med uppgiften att sköta planeringen och den operativa verksamheten för att upprätthålla och utveckla landets försörjningsberedskap. Försörjningsberedskapscentralen har till uppgift att

- utveckla samarbetet mellan den offentliga förvaltningen och näringslivet i frågor som gäller försörjningsberedskapen,
- säkerställa funktionen hos sådana tekniska system som är livsviktiga med tanke på försörjningsberedskapen,

- trygga kritisk varu- och tjänsteproduktion samt sådan produktion som stöder det militära försvaret,
- sköta den obligatoriska upplagringen och skyddsupplagringen,
- hålla material i statens säkerhetsupplag.

Institutet för hälsa och välfärd (THL)

Institutet för hälsa och välfärd har en styrningsroll inom den riksomfattande utvecklingen av informationsförvaltningen. THL utfärdar bland annat föreskrifter om systemkrav, allvarliga incidenter och anmälningen av dessa samt planen för egenkontroll.

THL svarar för den operativa styrningen av informationsförvaltningen inom social- och hälsovården. THL styr social- och hälsovårdsproducenterna och apoteken så att de kan ansluta sig till tjänsterna och utveckla sina informationssystem. THL har ett brett samarbetsnätverk. I egenskap av statistikmyndighet svarar THL även för upprätthållandet och utvecklingen av statistik- och registerdatabaserna samt de nationella klassificeringarna.

Regionförvaltningsverken

Regionförvaltingsverkens allmänna beredskapsuppgifter inbegriper att

- samordna beredskapen och ordna anknytande samverkan, samordna beredskapsplaneringen,
- stödja kommunernas beredskapsplanering,
- ordna beredskapsövningar,
- främja säkerhetsplaneringen inom region- och lokalförvaltningen,
- stödja behöriga myndigheter då myndigheterna leder säkerhetssituationer i regionen och vid behov samordna deras verksamhet.

Regionförvaltningsverken har beredskap att göra upp en regional lägesbild i omfattande och långvariga störningssituationer under normala förhållanden.

Social- och hälsovårdsministeriet (SHM)

Social- och hälsovårdsministeriet ansvarar för den strategiska styrningen av informationshanteringen inom social- och hälsovården, lagstiftningen samt det internationella och tväradministrativa samarbetet. Social- och hälsovårdsministeriet leder, övervakar och samordnar även social- och hälsovårdens förberedelser för störningssituationer och undantagsförhållanden. Målet är att säkra befolkningens försörjning och funktionsförmåga under alla förhållanden. Vid ministeriet svarar en särskild beredskapsenhet för beredskapsärenden. Social- och hälsovårdsministeriets beredskapsenhet upprätthåller situationsledningsberedskapen för störningssituationer i förvaltningsområdet och ett fortlöpande joursystem.

SoteDigi Oy

SoteDigi Oy är ett utvecklingsföretag som främjar digitaliseringen och samordningen av social- och hälsovårdstjänsterna i Finland i samarbete med social- och hälsovårdsaktörerna. SoteDigi Oy grundades i samband med beredningen av landskaps- och vårdreformen.

SoteDigi fokuserar framför allt på att

- genomföra nya nationella digitala lösningar, projekt och anskaffningar inom social- och hälsovården
- med hjälp av digitala lösningar dämpa ökningen av social- och hälsovårdens utgifter
- utveckla en teknisk miljö där klienterna erbjuds bättre service på lika villkor i hela Finland.

Dataskydds- och informationssäkerhetsfrågor är en viktig del av digitaliseringen av social- och hälsovårdstjänsterna, och dessa beaktas särskilt vid utvecklingen av tjänsterna. Informationssäkerhetsteknisk testning är ett centralt element i SoteDigis systemutveckling. Strävan är att hitta sårbarheter i systemen redan innan de pilottestas och tas i bruk. Beredskapen för störningssituationer och kontinuitetshanteringen planeras tillsammans med it-leverantörerna och tjänsteproducenten (Vimana Oy) så att eventuella produktionsavbrott och följderna av dem kan minimeras på ett kostnadseffektivt sätt.

Statsrådets lägescentral

Statsrådets lägescentral sammanställer för statsrådet en lägesbild av säkerhetsincidenter inklusive cyberstörningar. Lägescentralen styrs av lagstiftningen om den.

Tillstånds- och tillsynsverket för social- och hälsovården (Valvira)

Valvira sköter många tillsyns- och verkställighetsuppgifter i anslutning till cybersäkerheten hos social- och hälsovårdsaktörerna.

Valvira upprätthåller till exempel ett register över yrkesutbildade personer inom hälso- och sjukvården och en roll- och attributinformationstjänst som grundar sig på uppgifterna i registret. På basis av registret avgörs bland annat vem som har rätt att få tillgång till uppgifterna i Kanta-tjänsterna.

Valvira ansvarar för tillsynen över säkerheten i fråga om produkter och utrustning för hälso- och sjukvård. Valvira övervakar att de väsentliga kraven på social- och hälsovårdens informationssystem uppfylls. I sin helhet gäller tillsynen samtliga produkter och utrustningar för hälso- och sjukvård som redan släppts på marknaden och underhållet av dessa. Utöver tillverkarnas anmälningsskyldighet har yrkespersoner inom social- och hälsovården skyldighet att anmäla en farlig situation som orsakats av produkter och utrustning

för hälso- och sjukvård till den övervakande myndigheten. Uppgiftshelheten överförs från och med den 1 januari 2020 till Säkerhets- och utvecklingscentret för läkemedelsområdet (Fimea), dock så att tillsynsuppgifterna enligt lagen om klientuppgifter kvarstår hos Valvira. Således ska till exempel anmälningar om farliga situationer i patientdatasystemen[14] utredas vid Valvira.

Valvira har även till uppgift att i samarbete med Försörjningsberedskapscentralen identifiera försörjningsberedskapskritiska objekt i fråga om produkter och utrustning för hälso- och sjukvård samt att göra åtgärdsförslag till social- och hälsovårdsministeriet.

En av Valviras beredskapsuppgifter i anslutning till cybersäkerhet är att i samarbete med social- och hälsovårdsministeriet sammanställa en lägesbild utifrån sina uppgifter. En central uppgift är även att styra och informera regionförvaltningsverken.

Vimana Oy

Landskapens IKT-servicecenter Vimana Oy grundades för att utveckla gemensamma och kostnadseffektiva IKT-tjänster och främja digitaliseringen.

Projekt

Forumet AKUSTI

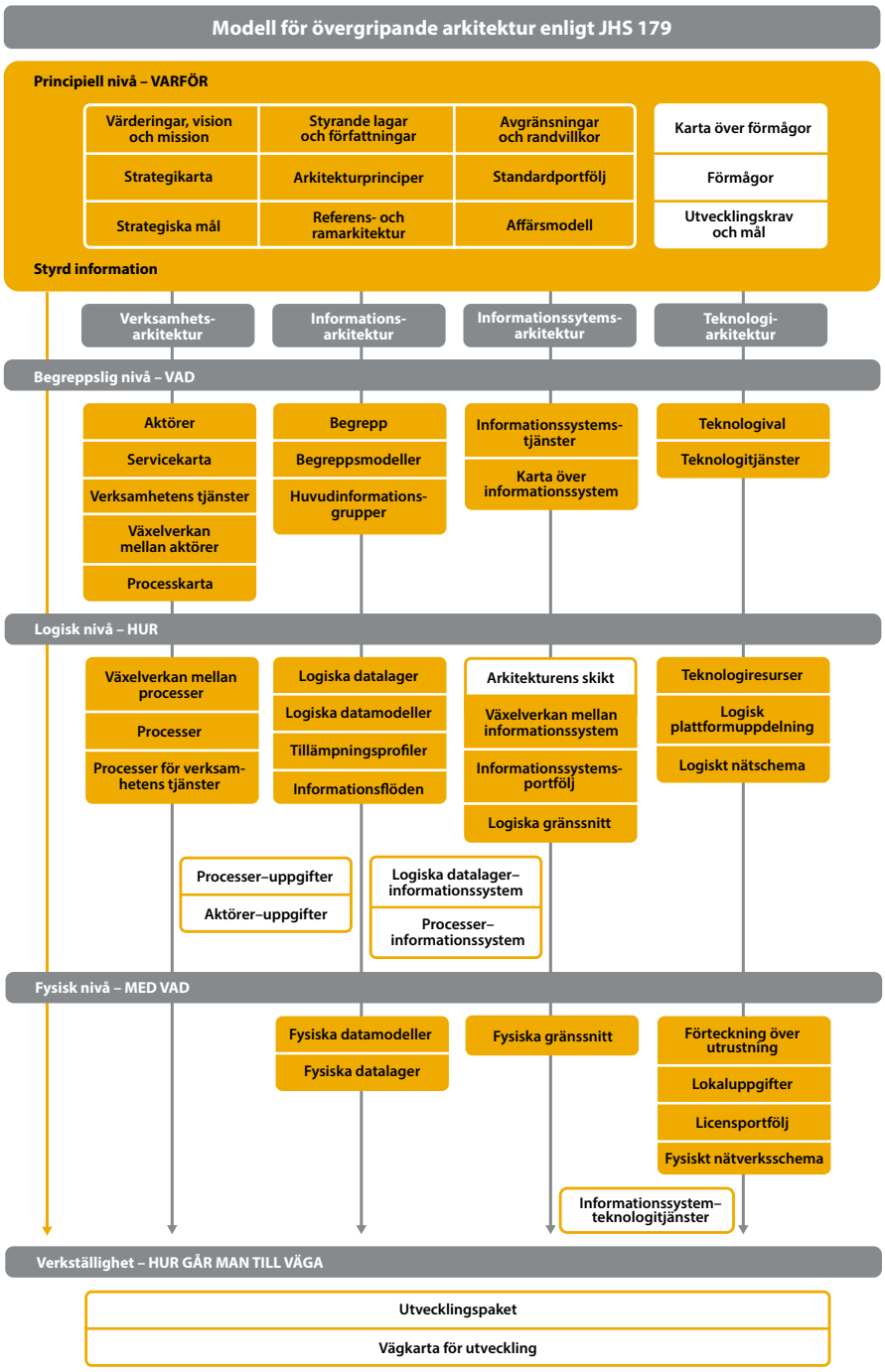
Forumet AKUSTI är ett nationellt samarbetsnätverk för informationsförvaltning inom social- och hälsovården som administrativt drivs via ett sekretariat vid Finlands Kommunförbund. Verksamheten finansieras av social- och hälsovårdsministeriet, universitetssjukvårdsdistrikten och kommunerna.

Utvecklingen av social- och hälsovårdstjänsterna och vårdstrukturerna förutsätter samarbete mellan kommunerna och sjukvårdsdistrikten samt mellan dessa och aktörerna inom statsförvaltningen när det gäller att ta fram lösningar för elektronisk informationshantering. AKUSTI deltar aktivt i planeringen och verkställandet av det nationella informationsförvaltningssamarbetet. Till forumets centrala uppgifter hör att främja verksamheten för social- och hälsovårdens övergripande arkitektur (SOTE KA) som stöd för social- och hälsovårdsministeriet. Målet med forumets verksamhet är bland annat att säkerställa att resultaten av den IKT-utveckling som redan utförts inom social- och hälsovården utnyttjas effektivt.

14 https://www.valvira.fi/terveydenhuolto/terveysteknologia/valviralle-tehtavat-ilmoitukset/ilmoitus-vaaratilanteesta

JHS 179

Delegationen för informationsförvaltningen inom den offentliga förvaltningen (JUHTA) har skapat en övergripande arkitekturmodell för JHS 179.



Figur 4. Referensram för arkitekturbeskrivningarna, JHS 179 (anpassad)

Rekommendationerna enligt JHS-systemet gäller informationshanteringen inom den statliga och kommunala förvaltningen. Till sitt innehåll kan JHS vara ett gemensamt förfarande, en definition eller en anvisning som avsetts för den offentliga förvaltningen. Målet med JHS-systemet är att förbättra kompabiliteten hos informationssystemen och uppgifterna i dessa, skapa förutsättningar för utveckling av funktioner oberoende av förvaltnings- och sektorsgränser samt effektivisera utnyttjandet av befintlig information.

Projektet om cyberhälsa

Projektet om cyberhälsa ingår i Försörjningsberedskapscentralens program Cyber 2020, vars referensram är den nationella cybersäkerhetsstrategin. I projektet, som delvis finansieras av Försörjningsberedskapscentralen, deltar flera sjukvårdsdistrikt samt deras IKT-tjänsteleverantörer och Cybersäkerhetscentret. Projektet inleddes hösten 2017 och fortsätter fram till september 2019. Största delen av projektets resultat skapas av de medverkande sjukvårdsdistrikten och av deras IKT-tjänsteleverantörer.

Projektet syftar till att skapa och sprida funktionssätt och praxis för cybersäkerhet inom hälso- och sjukvården för att utveckla cybersäkerheten inom de försörjningsberedskapskritiska organisationerna. Det viktigaste målet är att utveckla beredskapen för cyberhot inom sjukvårdsdistrikten särskilt i fråga om de funktioner som är kritiska för patientvården.

Tre huvudteman är utbildning om cybersäkerhet för personalen i branschen, datateknisk observations- och reaktionsförmåga i fråga om informationssäkerhetsincidenter samt beaktandet av cybersäkerhetskrav i upphandlingen av utrustning och tjänster. I utvecklingen deltar bland annat samtliga universitetssjukvårdsdistrikt, och resultaten sprids i takt med att projektet framskrider till alla sjukvårdsdistrikt. Projektresultaten distribueras och kan begäras bland annat via gruppen för informationsutbyte inom social- och hälsovården (SOTE-ISAC) vid Cybersäkerhetscentret.

VAHTI

Finansministeriet tillsatte ledningsgruppen för informations- och cybersäkerheten inom statsförvaltningen (VAHTI) som samarbets-, berednings- och koordineringsorgan för organisationer med ansvaret för utvecklingen och styrningen av den digitala säkerheten inom den offentliga förvaltningen. VAHTIs ställning har bekräftats i statsrådets principbeslut om Finlands cybersäkerhetsstrategi från 2013 och om utvecklandet av informationssäkerheten inom statsförvaltningen från 2009. VAHTI spelar dessutom en central roll i genomföringen av verkställighetsprogrammet för cybersäkerhetsstrategin.

VAHTI främjar även digitaliseringen av den offentliga förvaltningen genom att upprätta och upprätthålla en ändamålsenlig referensram för säkerhetskrav. Detta inkluderar

granskningar, godkännanden och utvärderingar som har ett samband med säkerheten och IKT-verksamhetens kontinuitet samt främjandet av informations- och cybersäkerhetsövningar.

VAHTI strävar efter att förbättra statsförvaltningens funktioner genom att utveckla informationssäkerheten samt att göra det lättare att integrera informationssäkerheten som en permanent del av förvaltningen, ledningen och resultatstyrningen. VAHTI-anvisningarna omfattar samtliga delområden inom informationssäkerheten.

Informationssäkerhetsanvisningarna finns på adressen https://www.vahtiohje.fi (bl.a. ett pdf-dokument om hanteringen av informationssäkerhetsincidenter).

Tyngdpunkterna inom utvecklingsprogrammet för digital säkerhet inom den offentliga förvaltningen 2018–2021 är

utvecklingen av ledandet av digital säkerhet och riskhantering, personalens kompetens, utvecklingen av digital kompetens och medvetenhet samt utnyttjandet av ny teknik för att effektivt genomföra nya tjänster och digital säkerhet.

Vi rekommenderar att varje organisation inom den offentliga förvaltningen deltar i det gemensamma projektet för digital säkerhet som genomförs inom ramen för JUDO-projektet och inom vilket man ämnar utveckla samtliga fem delområden för digital säkerhet (riskhantering – verksamhetens kontinuitet och beredskap – informationssäkerhet – cybersäkerhet – dataskydd) under åren 2019–2021.

Mer information och anmälan: https://vrk.fi/osallistu-digiturva-yhteishankkeeseen

Mer information om JUDO-projektet https://vrk.fi/judo

Bilaga 2

Styrande lagstiftning

Ett flertal lagar och förordningar innehåller bestämmelser om digitalisering och informationshantering inom social- och hälsovården. Lagstiftningen styr behandlingen av kund-, klient- och patientuppgifter. Nedan finns en förteckning över den viktigaste lagstiftningen på området.

Beredskapslagen 1552/2011

Enligt beredskapslagen ska statliga myndigheter och inrättningar samt kommunerna säkerställa att deras uppgifter kan skötas så väl som möjligt också under undantagsförhållanden. Beredskapen säkerställs bland annat genom beredskapsplaner och förberedelser för verksamhet under undantagsförhållanden.

Arkivlagen 831/1994 och Arkivverkets anvisningar

Lagen och anvisningarna tillämpas på förvaring av journalhandlingar.

EU:s direktiv om nät- och informationssäkerhet 2016/1148, det s.k. NIS-direktivet

Direktivet utgör en viktig del av lagstiftningen om cybersäkerhet. Det innehåller bestämmelser om hur kontinuiteten i verksamheten ska tryggas för aktörer som tillhandahåller tjänster av kritisk betydelse för samhället. NIS-direktivet är direkt kopplat till kritisk infrastruktur och till den nationella försörjningsberedskapen. Hanteringen av omfattande cyberstörningar inbegriper rapportering till Valvira i enlighet med direktivet. Med stöd av NIS-direktivet är organisationer inom hälso- och sjukvården skyldiga att anmäla cyberstörningar och andra incidenter som äventyrar patienternas säkerhet till Valvira.

EU:s allmänna dataskyddsförordning 2016/679 (GDPR)

Dataskyddsförordningen är en ny lag som reglerar behandlingen av personuppgifter och som tillämpas i alla EU-länder sedan den 25 maj 2018. Förordningen kompletteras och preciseras genom nationell lagstiftning.

Lagen om patientens ställning och rättigheter 785/1992

Lagen innehåller bestämmelser om behandlingen av journalhandlingar och om sekretessen för de uppgifter som ingår i handlingarna.

Lagen om klientens ställning och rättigheter inom socialvården 812/2000

Lagen innehåller bestämmelser om klientens rättigheter i fråga om behandlingen av och sekretessen för klientens uppgifter.

Lagen om klienthandlingar inom socialvården 254/2015

Lagen innehåller bestämmelser om registrering av klientuppgifter inom socialvården och om skyldigheterna i anslutning till detta.

Lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården 159/2007

Lagen föreskriver om elektronisk behandling av klientuppgifter inom de offentliga och privata social- och hälsovårdstjänsterna och om riksomfattande informationssystemtjänster. Lagen innehåller bestämmelser om hemlighållande, utlämnande och arkivering av uppgifter och om klientens rätt att få information om de egna klientuppgifterna.

Lagen om sekundär användning av personuppgifter inom social- och hälsovården

Lagen (RP 159/2017 rd) träder i kraft i början av april 2019. Den förenhetligar lagstiftningen om utlämnande av hälsouppgifter och inför en ny tillståndsmyndighet som kan sammanställa och samköra anonymiserade hälsouppgifter utan ett separat tillståndsförfarande. I och med lagen får kund- och klientuppgifter inom social- och hälsovården samt andra personuppgifter med anknytning till hälsa och välfärd användas i större utsträckning än tidigare även för andra ändamål än deras primära användningsändamål. Målet är att göra tillståndsbehandlingen och samkörningen av uppgifter i olika register smidigare och snabbare. På så sätt kan man öka användningen av social- och hälsovårdsuppgifter vid forskning och utveckling.

Lagen om elektroniska recept 61/2007

Lagen innehåller bestämmelser om behandlingen av elektroniska recept och om patientens rätt till information. Lagen föreskriver om det receptcenter och receptarkiv som upprätthålls av Folkpensionsanstalten.

Lagen om ändring av lagen om produkter och utrustning för hälso- och sjukvård 936/2017 (RP 165/2017 rd)

Lagen innehåller ändringar på miniminivå av lagen om produkter och utrustning för hälso- och sjukvård (629/2010) som behövs för det första steget av det nationella genomförandet av EU-förordningarna om medicintekniska produkter.

Säkerhetsutredningslagen 726/2014

Syftet med lagen är att införa ett effektivt förfarande för att utreda personers och företags bakgrund. Med dess hjälp och som en del av skyddet av det allmänna intresset tryggas säkerheten samt funktionen hos infrastruktur som är av kritisk betydelse för ett fungerande samhälle. Det finns tre nivåer av säkerhetsutredningar av personer (begränsad, normal och omfattande).

EU-förordningar om medicintekniska produkter s.k. MD-förordningen 2017/745 och IVD-förordningen 2017/746

I förordningarna fastställs bestämmelser om utsläppande på marknaden, tillhandahållande på marknaden eller ibruktagande av medicintekniska produkter för användning på människor och tillbehör till sådana produkter i unionen. Målet är att förbättra säkerheten i fråga om medicintekniska produkter. Förordningen innehåller bland annat bestämmelser om skyldigheten för produkttillverkarna att hantera och minska de cybersäkerhetsrisker som förekommer i samband med produkterna. Förordningen börjar tillämpas stegvis från och med våren 2020. Förordningen förutsätter att medicintekniska produkter som innehåller programvara får en certifiering för cybersäkerhet innan de släpps ut på marknaden.

Social- och hälsovårdsministeriets förordning om journalhandlingar 298/2009

Förordningen tillämpas på upprättandet av journalhandlingar samt på förvaringen av dessa och annat material som hänför sig till vård och behandling.

Hälso- och sjukvårdslagen 1326/2010

Lagen innehåller bestämmelser om utlämnande av patientuppgifter mellan ett sjukvårdsdistrikt och hälsovårdscentraler med verksamhet i distriktets område samt om användningen av dessa uppgifter.

Dataskyddslagen

Den nya dataskyddslagen om behandling av personuppgifter trädde i kraft den 1 januari 2019. Genom lagen kompletteras EU:s allmänna dataskyddsförordning.

Andra styrande dokument

Nationell riskbedömning 2018

Inre säkerhet. Inrikesministeriets publikationer 2019:5.

Säkerhetsstrategi för samhället, statsrådets principbeslut 2017

Principbeslutet om en säkerhetsstrategi för samhället bygger på samverkansmodellen för den övergripande säkerheten. Strategin förenhetligar de nationella principerna för beredskapen och styr förvaltningsområdenas beredskap.

Statsrådets beslut om målen med försörjningsberedskapen 2018

Tyngdpunkten i försörjningsberedskapsåtgärderna flyttas i allt högre grad mot säkerställande av den väsentliga infrastrukturens funktion vid sidan av materiell beredskap. Särskilda prioritetsområden när det gäller att trygga den kritiska infrastrukturens funktion är tryggande av energiförsörjningen, beredskap inför cybersäkerhetshot och stöd för återhämtning från dem, säkerställande av att det digitala samhällets datasystem, kommunikationstjänster och kommunikationsnät fungerar, tryggade lägesbestämnings- och tidsdatasystem samt fungerande logistiktjänster och nät.

Strategin för cybersäkerheten i Finland och dess verkställighetsprogram för 2017–2020

I verkställighetsprogrammet för strategin för cybersäkerheten i Finland 2017–2020 granskas utvecklingen av cybersäkerheten i fråga om de tjänster som erbjuds av staten, landskapen, kommunerna, företagen och tredje sektorn.

Institutet för hälsa och välfärds föreskrifter om harmonisering av kraven på informationshanteringen inom social- och hälsovården

De väsentliga kraven på informationssystem och informationshanteringslösningar harmoniseras på nationell nivå. Harmoniseringen och föreskrifterna i anslutning till den gäller lösningarnas funktion, interoperabilitet och informationssäkerhet https://thl.fi/fi/web/tiedonhallinta-sosiaali-ja-terveysalalla/maaraykset-ja-maarittelyt/maaraykset (på finska)

Utbildningsmaterial: https://www.slideshare.net/THLfi/tietoturvan-ja-tietosuojan-omavalvonta-suunnitelma-ja-toteuttaminen-131218 (på finska).

Valviras föreskrifter

Valvira publicerar föreskrifter och anvisningar som riktar sig till aktörer inom social- och hälsovården. https://www.valvira.fi/web/sv/publikationer-och-foreskrifter

VAHTI (ledningsgruppen för digital säkerhet inom den offentliga förvaltningen), som tillsatts av finansministeriet, utvecklar och styr den digitala säkerheten inom statsförvaltningen. Vahtis arbete omfattar alla delområden av informationssäkerheten. https://vm.fi/vahti

BILAGA 3

Begrepp

Anmälan om farlig situation – utöver tillverkarnas anmälningsskyldighet har yrkespersoner inom social- och hälsovården skyldighet att anmäla en farlig situation som orsakats av produkter och utrustning för hälso- och sjukvård (medicintekniska produkter) till den övervakande myndigheten Valvira så fort som möjligt.

Beredskap – verksamhet för att säkerställa att uppgifter kan skötas så störningsfritt som möjligt samt åtgärder som kan behöva vidtas i störningssituationer eller undantagsförhållanden och som avviker från det normala. Exempel på beredskapsåtgärder är beredskapsplanering, kontinuitetshantering, förhandsåtgärder, utbildning och beredskapsövningar.

Beredskapsplanering – planering av beredskap under normala förhållanden. Myndigheterna har enligt 12 § i beredskapslagen (1552/2011) skyldighet att vidta förberedelser bland annat genom beredskapsplanering. Vid beredskapsplaneringen utreds bland annat störningarnas och undantagsförhållandenas inverkan på organisationens uppgifter och verksamhet, vilka förändringar som sker i verksamheten och uppgifterna, hur verksamhetens kontinuitet kan tryggas och vilka åtgärder som krävs för att återgå till normala förhållanden. En viktig del av beredskapsplaneringen är att göra upp en beredskapsplan.

CERT-FI-gruppen (Computer Emergency Response Team) – CERT-FI-gruppen verkar inom Cybersäkerhetscentret vid Transport- och kommunikationsverket (Traficom) och har i uppgift att förebygga, observera och åtgärda säkerhetsöverträdelser i samband med nät-, kommunikations- och mervärdestjänster, att informera om hot mot informationssäkerheten och om informationssäkerhetsfrågor samt att samla in information.

Cyberhot – skadlig händelse eller utvecklingsgång som eventuellt realiseras och drabbar cybermiljön, och som när den realiseras äventyrar en funktion som är

beroende av cybermiljön. Förutom att cyberhot kan uppstå till följd av ett realiserat hot mot informationssäkerheten kan de även orsakas av handlingar i den digitala kommunikationsmiljön som äventyrar samhällets säkerhet. Cyberhot kan direkt eller indirekt riktas mot samhällets vitala funktioner, nationell kritisk infrastruktur eller medborgarna. De kan ha sitt ursprung inom landet eller utanför landets gränser.

Cybermiljö – verksamhetsmiljö som består av ett eller flera digitala informationssystem.

Cyberstörningssituation; störningssituation i cybersäkerheten; cyberstörning – ett cyberhot som realiserats och som är till skada för en organisations eller ett systems verksamhet.

Cybersäkerhet – tillstånd som eftersträvas där cybermiljön är tillförlitlig och verksamheten tryggas. Cybersäkerhet omfattar åtgärder genom vilka man på ett föregripande sätt kan kontrollera och vid behov stå emot olika cyberhot och deras konsekvenser. Störningar i verksamhet i en cybermiljö orsakas ofta av ett realiserat hot mot informationssäkerheten, varför informationssäkerheten spelar en central roll i strävan efter cybersäkerhet. Förutom genom informationssäkerhet försöker man även uppnå cybersäkerhet bland annat med hjälp av åtgärder som syftar till att trygga funktioner i den fysiska världen som är beroende av den cybermiljö som drabbats av en störning. Medan informationssäkerhet avser uppgifters tillgänglighet, integritet och konfidentialitet innebär cybersäkerhet säkerhet i fråga om ett samhälle eller en organisation som bygger på digitalisering och nätverk samt säkerhetens inverkan på olika funktioner. De centrala mål och riktlinjer med vars hjälp Finland svarar på utmaningar som riktas mot cybermiljön och säkerställer att den fungerar fastställs i strategin för cybersäkerheten i Finland (statsrådets principbeslut av den 24 januari 2013).

Cybersäkerhetscentret – Cybersäkerhetscentret vid Transport- och kommunikationsverket har i uppgift att övervaka hot mot cybersäkerheten och sammanställa information om cybersäkerhet för olika aktörer. Centret varnar för större cyberhot och riktar även upplysning till medborgarna. Cybersäkerhetscentret verkar både inom den offentliga och privata sektorn. Centret tillhandahåller effektiviserade tjänster för försörjningsberedskapskritiska organisationer, däribland många organisationer inom social- och hälsovården.

Hantering av informationssäkerhetsincidenter, hantering av it-incidenter, it-incidenthantering – åtgärder genom vilka man förbereder sig inför och reagerar på it-säkerhetsincidenter i syfte att begränsa skadorna och återhämta sig från dem.

Hybridpåverkan – politiskt motiverad, planmässig verksamhet, genom vilken man försöker nå de egna målen med hjälp av olika medel som kompletterar varandra och genom att utnyttja svagheter hos det objekt som är föremål för verksamheten. Vid hybridpåverkan

kan exempelvis ekonomiska, politiska eller militära medel användas. Medlen kan användas samtidigt eller efter varandra. Hybridpåverkan sker bland annat genom informations- och cyberåtgärder samt fysiska och ekonomiska åtgärder. Både statliga och icke-statliga aktörer kan ligga bakom hybridpåverkan.

ICMT (Information, Communication and Medical Technology) Allmän term som beskriver teknologi som är knuten till medicinteknisk utrustning.

Identifiering, identifikation, igenkänning – förfarande för att med säkerhet identifiera en person, ett föremål eller ett ärende.

Informationssäkerhet, it-säkerhet – arrangemang som syftar till att säkerställa informationens tillgänglighet, integritet och konfidentialitet. Tillgänglighet innebär att informationen kan utnyttjas vid önskad tidpunkt. Med integritet avses informationens överensstämmelse med den ursprungliga informationen och med konfidentialitet att informationen inte är tillgänglig för utomstående. Informationssäkerhetsarrangemang är till exempel passerkontroll, låsning av utrymmen, säker förvaring och förstöring av dokument, kryptering och säkerhetskopiering av data samt användning av brandvägg, antivirusprogram och certifikat. Till informationssäkerheten hör bland annat säkerställandet av informationsmaterial, utrustning, programvara, telekommunikation och verksamhet.

Informationssäkerhetsincident, it-säkerhetsincident, it-incident – en eller flera sammanhängande, oväntade eller oönskade informationssäkerhetshändelser, som äventyrar uppgifters och tjänsters informationssäkerhet och har en negativ inverkan på en organisations verksamhet.

Integritetsskydd; skydd för personuppgifter – arrangemang med vilka man strävar efter att säkerställa att personuppgifter behandlas på ett korrekt sätt så att uppgifternas sekretess bevaras.

Kontinuitetshantering – process i en organisation med vars hjälp man identifierar hot mot verksamheten och bedömer vilka konsekvenser de får för organisationen och dess aktörsnätverk samt skapar rutiner för att hantera störningssituationer och säkerställa kontinuiteten i verksamheten i alla förhållanden.

Kritisk infrastruktur – grundläggande strukturer, tjänster och relaterade funktioner som är nödvändiga för att upprätthålla samhällets vitala funktioner.

Ledningsgruppen för digital säkerhet inom den offentliga förvaltningen VAHTI – organ inom statsförvaltningen som behandlar och samordnar statsförvaltningens centrala riktlinjer för informations- och cybersäkerheten (VAHTIs anvisningar).

Nationell kriteriesamling för säkerhetsauditering (Katakri) – ett utvärderingsverktyg som kan användas av myndigheter för att utvärdera en organisations kapacitet att skydda myndighetens säkerhetsklassificerade information.

Normala förhållanden – det vanliga tillståndet i samhället där samhällets vitala funktioner kan tryggas utan att myndigheterna behöver ges möjlighet att utöva befogenheter som avviker från det normala. Även om det inträffar störningar i samhället är det fråga om normala förhållanden så länge som inte statsrådet i samverkan med republikens president konstaterar att undantagsförhållanden råder. Under normala förhållanden kan hot förebyggas eller vid behov avvärjas inom ramen för myndigheternas regelrätta befogenheter och resurser samt företagens normala riskhanteringsmetoder. De system och andra åtgärder som byggs upp under normala förhållanden lägger grunden för agerandet vid störningar och under undantagsförhållanden.

Nätövervakningscentral, nätverksoperationscenter – organisation eller del av organisation där man administrerar och övervakar ett eller flera nätverk.

Resiliens – enskilda individers och sammanslutningars förmåga att upprätthålla funktionsförmågan under föränderliga förhållanden och deras beredskap att möta störningar och kriser och att återhämta sig från dem.

Riskanalys – åtgärder för att identifiera riskerna och bedöma sannolikheten för ett skadefall samt de förväntade skadorna. Olika metoder kan användas vid en riskanalys beroende på objekt, verksamhet och situation. Med skadefall avses en händelse som leder till att skada uppstår, dvs. skadlig förlust.

Riskhantering – systematisk verksamhet som inkluderar riskanalys samt planering, genomförande och uppföljning av nödvändiga åtgärder samt korrigerande åtgärder. En plan för egenkontroll (en informationssäkerhetsplan) är av central betydelse för riskhanteringen. I riskhanteringsmedel ingår riskeliminering, risköverföring, riskreducering genom att dela riskerna och bekämpa skadorna samt behållande av risk. Inom beredskap är riskhantering ett samarbete mellan flera olika aktörer, såsom företag, olika sektorer och myndigheter, kommuner och staten. Myndigheter och vissa företag har en lagstadgad skyldighet att göra upp beredskapsplaner av vilka riskhantering utgör en viktig del. Till riskhanteringen hör också dimensionering av tillräckliga resurser.

Samhällets vitala funktioner – funktion som är nödvändig för att samhället ska fungera.

Störningssituation – hot eller händelser som äventyrar samhällets vitala funktioner eller strategiska uppgifter och som kräver mer omfattande eller intensivare samarbete och kommunikation mellan myndigheter och andra aktörer för att man ska kunna kontrollera

dem. Störningssituationer är till exempel allvarliga naturkatastrofer eller störningssituationer som orsakas av mänskligt agerande. Störningssituationer kan förekomma under såväl normala förhållanden som undantagsförhållanden. En störningssituation kan vara riksomfattande, regional eller lokal. En störningssituation kan också gälla en specifik funktion.

Sårbarhet – utsatthet för hot som riktas mot informationssäkerheten. Sårbarhet kan vara vilken svaghet som helst som gör att en skada kan uppkomma eller som kan användas för att orsaka en skada. Sårbarhet kan förekomma i informationssystem, processer och människors verksamhet.

Säkerhetsoperationscenter – organisation eller del av organisation där man skapar, följer och analyserar en lägesbild av informationssäkerheten samt förebygger, identifierar och analyserar informationssäkerhetsincidenter, dokumenterar dem och reagerar på dem i enlighet med anvisningarna.

Säkerhetsoperationscenter (security operations centre, SOC) – organisation eller del av organisation där man skapar, följer och analyserar en lägesbild av informationssäkerheten samt förebygger, identifierar och analyserar informationssäkerhetsincidenter, dokumenterar dem och reagerar på dem i enlighet med anvisningarna. En organisation kan ha ett eget säkerhetsoperationscenter eller så kan tjänsterna köpas av en utomstående tjänsteleverantör.

Säkerhetsutredning – Skyddspolisens eller försvarsmaktens utredning av en persons bakgrund eller av bakgrunden hos ett företags ansvarspersoner samt företagets informationssäkerhetsnivå och förmåga att sköta åtaganden.

Säkerhetsöverträdelse, kränkning av informationssäkerheten – att vidta obehöriga åtgärder i fråga om information eller informationssystem. De vanligaste säkerhetsöverträdelserna är missbruk av användarnamn och lösenord, dataintrång, nedsmittning med skadligt program, överbelastningsangrepp, informationsstöld och riktade sabotageprogram.

Undantagsförhållanden – en i beredskapslagen (1552/2011) avsedd situation i samhället där det förekommer så många eller allvarliga störningar eller hot att det är nödvändigt att ge myndigheterna möjlighet att utöva befogenheter som avviker från det normala. Statsrådet konstaterar i samverkan med republikens president att undantagsförhållanden råder.

Utpressningsprogram – skadligt program som krypterar eller manipulerar filer i en dator och normalt kräver att användaren betalar en lösensumma för att krypteringen ska hävas.

Utredning av säkerhetsöverträdelse – åtgärder som vidtas när en säkerhetsöverträdelse upptäcks i syfte att reda ut överträdelsen. En utredning av säkerhetsöverträdelse

kan bland annat innebära säkring av bevismaterial, kriminalteknik, analys av skadligt program, logganalys eller en allmän utredning av säkerhetsöverträdelsens konsekvenser och omfattning.

Åtkomstkontroll – förfaranden för att bevilja, neka eller på annat sätt hantera åtkomsten till tjänster och systemresurser.

Överbelastningsangrepp – it-angrepp i syfte att belasta och därmed lamslå en tjänst eller ett informationssystem.

Källa

Säkerhetskommittén, Ordlista om cybersäkerhet 2018
Säkerhetskommittén och Terminologicentralen TSK: Ordlista om övergripande säkerhet 2017

BILAGA 4

För- och nackdelar med ett distribuerat respektive centraliserat system

Genom att bevara kopior av informationssystemets infrastruktur på olika ställen kan man effektivt hantera fysiska hot och även vissa digitala och samhälleliga hot. Exempel på sådana hot är eldsvådor, störningar i telekommunikationen och arbetskonflikter. Genom att distribuera systemet skapas på ett naturligt sätt punkter som systemets interna telekommunikation koncentreras till. Detta bidrar till att förhindra digitala hot, såsom spridningen av skadliga program.

För att de delar av informationssystemet som finns utspridda på olika ställen ska vara synkroniserade krävs det stor noggrannhet. Den enklaste lösningen kan vara att sammankoppla de olika it-utrymmena med en VPN-anslutning, varvid datorerna förefaller att höra till samma intranät trots att de är placerade långt från varandra. I detta fall kan samma metoder användas vid synkroniseringen som vid synkronisering av parallella datorer som finns i ett och samma it-utrymme.

Om organisationens verksamhet klarar av smärre avbrott i informationssystemets funktion kan det som beredskap räcka att det finns en kopia av systemet, även om den inte är i drift.

Ju sämre verksamheten tål avbrott desto viktigare är det att se till att de olika delarna i ett distribuerat system är synkroniserade och att användaren inte märker om den del av

systemet som betjänar användaren byts ut. Ofta räcker det att endast vissa delar av systemet, till exempel databasen, hela tiden är synkroniserade medan beredskapen i fråga om andra delar kan vara långsammare.

Övervakningen av funktionen och säkerheten hos ett distribuerat system kräver ofrånkomligen övervakning av fler detaljer än när det är fråga om ett centraliserat system. Goda förberedelser minskar det efterföljande arbetet eftersom även övervakningen då kan automatiseras.

BILAGA 5

Certifiering och auditering av system samt standarder

institutet för hälsa och välfärds föreskrifter om informationshantering inom social- och hälsovården https://thl.fi/fi/web/tiedonhallinta-sosiaali-ja-terveysalalla/maaraykset-ja-maarittelyt/maaraykset (på finska)

Katakri – nationell kriteriesamling för säkerhetsauditering

Katakri ett utvärderingsverktyg som kan användas av myndigheter för att utvärdera en organisations kapacitet att skydda myndighetens sekretessbelagda information. Katakri innehåller minimikrav som grundar sig på nationella författningar och internationella förpliktelser. Kraven utgör inte anvisningar om genomförandet och är inte heller i sig säkerhetskrav vid upphandling. Alla krav behöver inte tillämpas på alla system som granskas.

Det huvudsakliga syftet med Katakri är att förenhetliga myndighetsfunktionerna när en myndighet genomför en auditering av ett objekts säkerhetsnivå i ett företag eller någon annan sammanslutning. Organisationer kan även använda delar av Katakri som riktlinjer när de utvecklar informationssäkerheten i sin verksamhet. Katakri innehåller ett stort antal hänvisningar till ISO/IEC 27000-standarder. Den senaste versionen av Katakri är från 2015.

ITIL (IT Infrastructure Library)

Ramverket ITIL är en sammanställning av bästa praxis inom hanteringen av it-tjänster. AXELOS äger rättigheterna till modellen och publicerar dokument med anknytning till ITIL. ITIL definierar processer, roller och funktioner i samband med tillhandahållande av tjänster. ITIL är utformat för att täcka it-tjänsternas hela livscykel:

- tjänstestrategi

- tjänstedesign
- tjänsteöverlämning
- tjänstedrift
- kontinuerlig tjänsteförbättring.

COBIT 5

COBIT 5 är en internationell företagsarkitekturmodell för it-styrning som inkluderar principerna för utveckling av informationssäkerheten. Närmare information om arkitekturmodellen finns på ISACANs webbplats www.isaca.org

STANDARDER

Standarderna utgör en referensram och stomme för den långsiktiga utvecklingen av verksamheten. Nedan finns en förteckning över ett antal standarder och referensramar som är viktiga inom hälso- och sjukvården. ISO/IEC-standarderna är välkända i Finland och inkluderar ledning av informationssäkerhet.

Ledningssystemet för informationssäkerhet:

- är en del av det allmänna ledningssystem som planeras och genomförs utifrån en bedömning av affärsriskerna
- används, övervakas, granskas, upprätthålls och förbättras i syfte att åstadkomma större informationssäkerhet
- underlättar organiseringen av informationssäkerhetsarbetet för företagsledningen
- bör omfatta alla förfaranden och åtgärder som behövs vid styrningen, förvaltningen och övervakningen av informationssäkerheten
- är inte ett enskilt dokument, utan en process i många delar som kräver kontinuerlig utveckling
- består bland annat av en riskanalys och en informationssäkerhetspolicy samt planer för informationssäkerhet, kontinuitet och återhämtning
- ISO/IEC 27000 avser den växande standardfamiljen ISO/IEC med den gemensamma rubriken ”Informationsteknik. Säkerhetstekniker. Ledningssystem för informationssäkerhet”
- ger rekommendationer som gäller ledning, risker och kontroll i fråga om informationssäkerhet i ledningssystem för informationssäkerhet
- även andra 27-standarder om informationssäkerhet anses ibland höra till familjen.

Innehåll i standardfamiljen ISO 27000 (innehåll av störst betydelse för hälso- och sjukvården):

- 27000:2015 - Översikt och terminologi
- 27001:2013 - Krav
- 27002:2013 - Riktlinjer för informationssäkerhetsåtgärder
- 27003: 2010 - Vägledning för införande av ledningssystem för informationssäkerhet
- 27004:2009 - Mätning
- 27005:2011 - Riskhantering för informationssäkerhet
- 27799:2016 - Hälso- och sjukvårdsinformatik. Ledningssystem för informationssäkerhet i hälso- och sjukvården baserat på ISO/IEC 27002.

Standarden ISO 22301 behandlar organisationens kontinuitetshantering bland annat med tanke på cybersäkerheten.

Ytterligare stödmaterial:

FINLANDS STANDARDISERINGSFÖRBUND SFS SFS-EN ISO/IEC 27002:2017
FINNISH STANDARDS ASSOCIATION SFS 3
Informationsteknik. Säkerhetstekniker. Riktlinjer för informationssäkerhetsåtgärder
Information technology. Security techniques. Code of practice for information security controls (ISO/IEC 27002:2013 including Cor 1:2014 and Cor 2:2015)

BILAGA 6

Riktlinjer för den offentliga förvaltningens molntjänster

Riktlinjerna för den offentliga förvaltningens molntjänster har utarbetats i enlighet med finansministeriets (FM) beslut FM/276/00.01.00.01/2018.

Riktlinjerna fastställer hur data som ägs av en organisation inom den offentliga förvaltningen kan behandlas i molntjänster. Syftet med riktlinjerna är att stödja staten, landskapen och kommunerna i beslutsfattandet när de planerar och anskaffar nya IKT-tjänster.

Riktlinjerna behandlar IKT-tjänster som tillhandahåller delade resurser (t.ex. datorkapacitet, lagrings-, säkerhetskopierings- och dataöverföringskapacitet), dvs. så kallade molntjänster. De nya informationssystemen och processerna utnyttjar i allt högre grad molntjänster. Fördelar med denna teknologi är att den är kostnadseffektiv, skalbar, informationssäker, energieffektiv, flexibel och innovativ. Molntjänsterna omfattar fem huvudsakliga servicemodeller: egen datacentral, egen datacentral som drivs av en utomstående tjänsteleverantör, infrastruktur som tjänst (IaaS), plattform som tjänst (PaaS) och mjukvara som tjänst (SaaS). De huvudsakliga realiseringsmodellerna är följande: egen datacentral, privat moln, offentligt mol och hybridmoln.

Riktlinjer:

1. Molntjänsterna ska behandlas som vilken annan anskaffning eller ändring av en IKT-tjänst som helst.
2. När det gäller molntjänster ska särskild uppmärksamhet fästas vid avtal, säkerställandet av tjänstens kontinuitet och tillgången till informationen.
3. Molntjänsten ska uppfylla den anskaffande partens krav på servicenytta och servicegaranti.
4. När molntjänsten eller molntjänstteknologin tillhandahåller den bästa servicenyttan och servicegarantin och det inte föreligger andra hinder ska den väljas i första hand.
5. Molntjänsternas servicenytta och servicegaranti ska bedömas regelbundet och när väsentliga avtalsvillkor ändras.
6. Behandlingen av offentlig information begränsas inte.
7. Icke-offentlig information kan behandlas i offentliga molntjänster när dataskyddet och datasäkerheten har tillgodosetts och verifierats på ett ändamålsenligt sätt.

BILAGA 7

Tekniska skyddsmetoder och andra anvisningar

Organisationerna inom social- och hälsovårdssektorn utsätts i dag för cyberattacker av mycket varierande slag. Nedan följer en sammanställning av anvisningar från olika offentliga källor, med särskilt fokus på det tekniska skyddet.

En av de viktigaste grundläggande åtgärderna för att skydda sig mot olika typer av skadliga program är att se till att mjukvaran är uppdaterad. Om exempelvis en dator eller mjukvara som är kopplad till medicinteknisk utrustning inte kan uppdateras på grund av utrustningens godkännanden, ska det runt utrustningen byggas upp ett separat skydd, till exempel med hjälp av nätsegmentering eller brandväggar.

EU:s byrå för nät- och informationssäkerhet (Enisa) har publicerat anvisningar om cybersäkerhet i smarta sjukhus: https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals

I Förenta staterna har det publicerats ett flertal anvisningar om cybersäkerhet i sjukhusmiljöer. NCCoE (National Cybersecurity Center of Excellence) vid det amerikanska NIST-institutet har 2018 bland annat publicerat anvisningar om sjukhusens it-miljö: https://www.nist.gov/programs-projects/security-health-information-technology

Det finns även särskilda anvisningar om exempelvis tryggande av infusionspumpar: https://www.nccoe.nist.gov/sites/default/files/library/sp1800/hit-wip-nist-sp1800-8.pdf

Därtill finns det anvisningar om skydd av hälsouppgifter på bärbara enheter: https://www.nccoe.nist.gov/sites/default/files/library/sp1800/hit-ehr-nist-sp1800-1.pdf

HelseCERT i Norge har skrivit tekniska anvisningar för användarna om underhåll och härdning av systemen. https://www.nhn.no/helsecert/anbefalte-sikkerhetstiltak/

Mobila enheter och deras informationssäkerhet

Mobila enheter som hör till ett sjukhus avlägsnas från sjukhuset bland annat i en situation där en kund eller en anställd inom social- och hälsovården med en mobil enhet registrerar hälsouppgifter antingen via ett moln eller direkt i en tjänst via sjukhusets intranät. Ett skydd som har visat sig fungera bra är att skapa en separat APN-adress (access point name) för varje tjänst. I samarbete med teleoperatören kan tjänsten begränsas så att den bara syns via den aktuella APN-adressen i enheter som använder internet. När man dessutom på förhand gör en noggrann bedömning av behovet av telekommunikation och

ställer in tjänstens övriga allmänna skydd (t.ex. brandväggen och kontrollen av avvikelser) på lämpligt sätt, kan risken för störningar och missbruk sänkas till en acceptabel nivå.

De mjukvaror och tjänster som ingår i Microsoft Office 365, exempelvis e-post, kan i princip även användas på mobila enheter. Många applikationer för mobila enheter stöder emellertid inte identifiering av användaren med hjälp av multifaktorautentisering. Till exempel stöder inte e-postapplikationen i Apple iOS multifaktorautentisering.

Brottslingar försöker mycket aktivt komma över användarnas användarnamn och lösenord för att därefter göra intrång i en organisations datasystem med hjälp av lösenorden och applikationer som inte stöder multifaktorautentisering. Om en organisation tillåter att de anställda loggar in i tjänster utan multifaktorautentisering tillåter den det även för brottslingar. Organisationer som använder Office 365-produkter måste således välja mellan att förbjuda användningen av applikationer med sämre informationssäkerhet eller att ta risken att utsättas för dataintrång.

De anställdas rutiner för att använda systemen (lösenordspraxis, gemensamma inloggningsuppgifter)

Den som använder informationssystem ska i regel identifiera sig i systemen med sitt personliga användar-id. Ett system med samlad inloggning rekommenderas så att användarna inte behöver komma ihåg flera olika användarnamn och lösenord.

I regel bör man inte tillåta att flera personer delar och använder samma inloggningsuppgifter. Användarorganisationen kan dock tillåta gemensamma inloggningsuppgifter i fråga om system och anordningar som inte behandlar känsliga uppgifter, som inte stöder flera användar-id och som ska skyddas från andra än personalen. En sådan anordning kan exempelvis vara ultraljudsutrustning som är placerad i korridoren i sjukhusets poliklinik.

I regel ska informationssystem inte kunna användas utan att användaren identifierar sig. Användarorganisationen kan godkänna att en anordning används utan identifiering om den inte behandlar några känsliga uppgifter och den är fysiskt skyddad mot missbruk. En sådan anordning kan exempelvis vara ultraljudsutrustning som är placerad i ett låst mottagningsrum.

Fjärråtkomst för anordnings- och systemleverantörer

De tekniska kraven i fråga om fjärråtkomst och det sätt som fjärråtkomst får användas på bör fastställas redan när ett avtal ingås, så att systemleverantören förbinder sig att följa den verksamhetsmodell som sjukhuset vill ha. Samma typ av fjärråtkomst lämpar sig inte för alla leverantörer, vilket sjukhuset måste acceptera. Det väsentliga är att

nätverksövervakningen, SOC eller någon annan motsvarande aktör kan identifiera tillåtna och otillåtna fjärråtkomster i internettrafiken. Det här är svårt att åstadkomma till hundra procent.

Spridning av skadliga program (utpressningsprogrammet WannaCry)

För att kunna förhindra att datorvirus, dvs. skadliga program, smittar och sprids krävs det framför allt att datoranvändarna agerar på ett säkert sätt, att mjukvaran är uppdaterad och säker och att antivirusprogram används. Om skadliga program kommer åt att smitta en dator kan en spridning begränsas genom att nätverken segmenteras, de enheter som är kopplade till nätet identifieras och användarrättigheterna för användarna och processerna begränsas.

Nätverkssegmentering innebär att helheter som används för olika ändamål åtskiljs från varandra på galvanisk väg med hjälp av separata ledningar och nätverksenheter, med åtgärder för att separera nätverksenheterna (t.ex. VLAN), med brandväggar eller en kombination av dessa. Till exempel bör man alltid hålla medicinteknisk utrustning, datorer som används i patientvården och datorer som används för vanligt kontorsarbete åtskilt från varandra. På många sjukhus är så inte fallet – nätverken är ofta stora med en platt nätverksarkitektur. I ett sådant nätverk finns det inget som hindrar en smittad dator från att vara i kontakt med andra datorer.

Enheter som är kopplade till nätet identifieras med hjälp av certifikat. I praktiken kontrolleras anslutna enheter sällan.

Skrivrättigheterna till delade resurser för enheternas applikationer och användare bör kartläggas ännu noggrannare och begränsas ytterligare. Användarna och applikationerna ges ofta omfattande skrivrättigheter. Detta ökar de skador som orsakas av skadliga program som krypterar filer.

Nyttiga anvisningar för organisationer inom social- och hälsovården (anvisningar från Cybersäkerhetscentret vid Traficom och VAHTI):

Selviytymisopas kiristyshaittaohjelmia vastaan - Kokemuksia kiristyshaittaohjelmista Suomessa ja neuvoja niistä selviytymiseen (005/2016 J). https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kiristyshaittaohjelmat__teemakooste_07_2016.pdf

Lokien keräys ja käyttö - Ohje lokitietojen tallentamiseen ja hyödyntämiseen (Ohje 4/2016). https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Lokitusohje.pdf

Palvelunestohyökkäysten ehkäisy ja torjunta (Ohje 3/2016). Anvisningen behandlar framför allt hur offentliga www-tjänster kan skyddas mot överbelastningsangrepp. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Ohje_3_2016_Palvelunestohyokkaysten_ehkaisy_ja_torjunta.pdf

Verkkosivujesi pimeä puoli - Ohjeita sisällönhallintajärjestelmien kyberuhkien torjumiseksi (Ohje 2/2016). https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Sisallonhallintajarjestelmien_kyberuhkia.pdf

Verkkopalvelun ohjelmistoalustan valinta ja palvelun turvallinen ylläpito (Ohje 1/2011). https://www.kyberturvallisuuskeskus.fi/fi/verkkopalvelun-ohjelmistoalustan-valinta-ja-palvelun-turvallinen-yllapito-ohje-12011

Terveydenhuoltoalan kyberuhkia (Ohje 1/2016). En kort översikt i fågelperspektiv för chefer i organisationer inom social- och hälsovården. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Terveydenhuoltoalan_kyberuhkia.pdf

Kohdistettujen haittaohjelmahyökkäyksien uhka on otettava vakavasti. Rapport som innehåller beskrivningar av riktade angrepp (engl. advanced persistent threat, APT) och anvisningar om hur man kan skydda sig mot dem. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kohdistetut_haittaohjelmahyokkaykset_uhka_otettava_vakavasti_raportti_28082014.pdf

Tietoturvavinkkejä matkapuhelimen turvalliseen käyttöön (Ohje 10/2014). Råd om hur mobiltelefoner kan användas och underhållas på ett cybersäkert sätt, kan även tillämpas på surfplattor. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Tietoturvavinkkeja_matkapuhelimen_turvalliseen_kayttoon.pdf

Langattomasti, mutta turvallisesti. Langattomien lähiverkkojen tietoturvallisuudesta (Ohje 2/2014). Råd till konsumenter och småföretag om hur WLAN/WiFi-nätverk kan användas och upprätthållas på ett cybersäkert sätt. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Langattomasti_mutta_turvallisesti._Langattomien_lahiverkkojen_tietoturvallisuudesta.pdf

Näin meitä huijataan! Verkossa yleisesti tavattuja huijausmenetelmiä (Ohje 1/2014) (uppdaterad 30.3.2017). Information om bedrägerier som sker via internet och råd om hur de kan undvikas samt anvisningar för den som har blivit lurad. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Nain_meita_huijataan.pdf

Salasanat haltuun - Neuvoja salasanojen käyttöön ja hallintaan (sammanställning av temat för december 2014). Råd om val, användning och hantering av lösenord för den som använder och tillhandahåller IKT-tjänster. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Salasanat_haltuun.pdf

Pilvipalvelujen turvallisuus. Mitä organisaatioiden tulisi huomioida pilvipalveluja hyödyntäessä (Ohje 5/2014). https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_tietoturva_organisaatioille.pdf

Kansainvälisesti toteutetun palvelun tietoturvasta tiedottaminen (Suositus 205/2014 S). Rekommendation om hur teleföretag bör informera sina beställare om informationssäkerheten när det gäller kommunikationstjänster som helt eller delvis genomförs utanför Finland. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/Suositus_205_2014.pdf

Toiminnan jatkuvuuden hallinta (VM:n julkaisuja 2/2016). http://urn.fi/URN:ISBN:978-952-251-779-1

Tietoturvapoikkeamatilanteiden hallinta (VM:n julkaisuja 8/2017). http://urn.fi/URN:ISBN:%20978-952-251-930-6

ICT-varautumisen vaatimukset (VAHTI 2/2012) https://www.vahtiohje.fi/web/guest/2/2012-ict-varautumisen-vaatimukset

Kuntaliitto
Kommunförbundet

Cybersäkerhet ingår i beredskapen för social- och hälsovårdens tjänster.

Denna anvisning syftar till att ge en överblick över de principer om cybersäkerhet som gäller sektorn samt de befintliga anvisningarna och rekommendationerna. Anvisningen grundar sig på verkställighetsprogrammet för strategin för cybersäkerheten i Finland och bidrar till att säkerställa samhällets vitala funktioner i störningssituationer.

Anvisningen innehåller inte detaljerade eller tekniska åtgärder för att identifiera eller avvärja cyberhot, utan i dessa frågor kan aktörerna vända sig till bland annat Cybersäkerhetscentret för handledning. Även exempelvis Institutet för hälsa och välfärd har tagit fram definitioner, föreskrifter och utbildningsmaterial för informationshanteringen i branschen.

Det är fråga om en allmän anvisning för social- och hälsovårdsaktörerna i olika organisationer som har beretts inom ramen för social- och hälsovårdsministeriets och Kommunförbundets gemensamma projekt.

En första version av anvisningen publiceras i social- och hälsovårdsministeriets publikationsserie och kommer att uppdateras efter behov. Bilagorna innehåller bakgrundsuppgifter och fördjupande information.

Internet: stm.fi/sv/publikationer

BESTÄLLNINGAR:
julkaisutilaukset.valtioneuvosto.fi

ISSN PDF 1797-9854
ISBN PDF 978-952-00-4092-5