Turvallisuuskomitea
Säkerhetskommittén
The Security Committee

STRATEGI FÖR CYBERSÄKERHETEN I FINLAND 2019

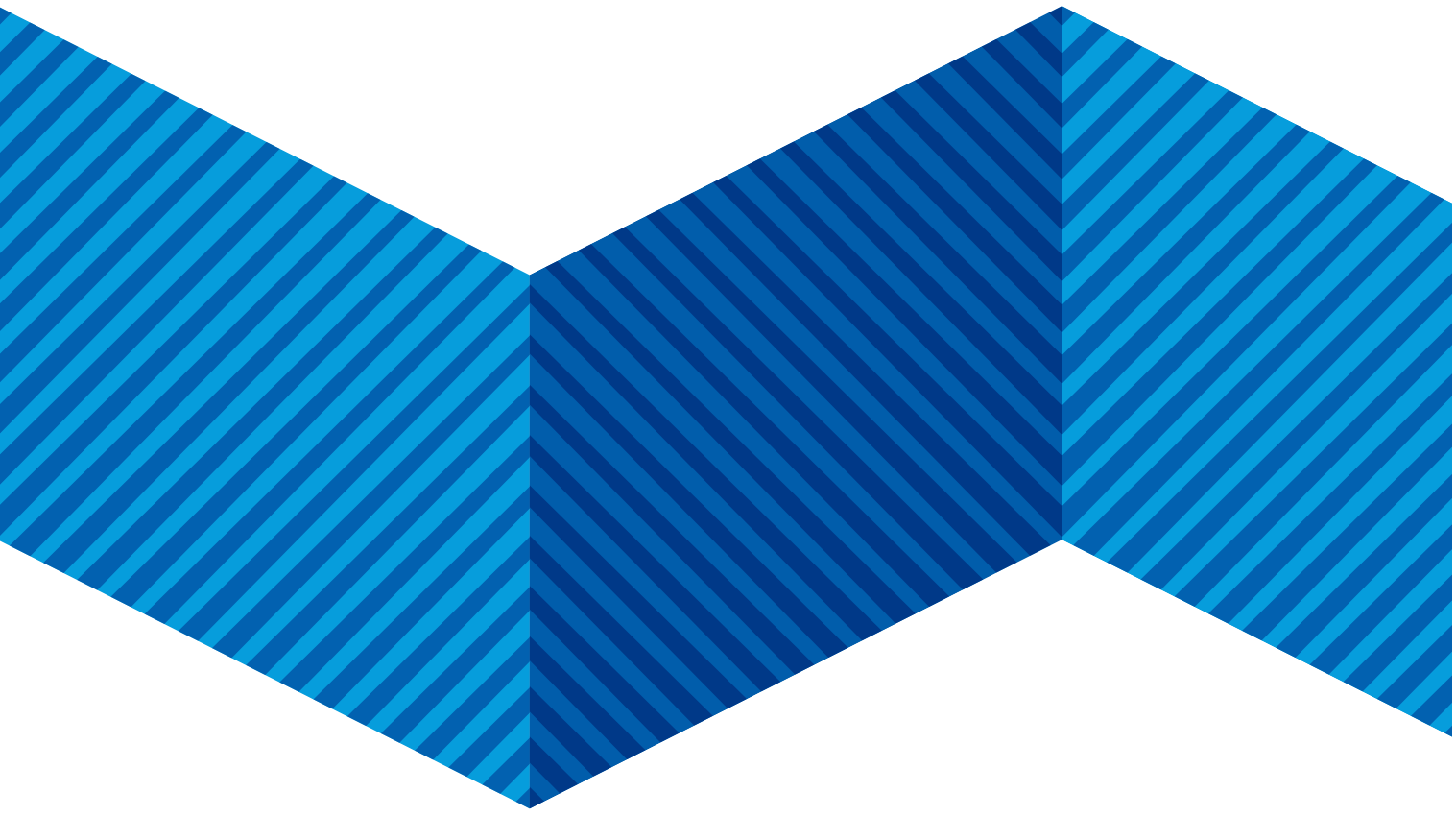
Statsrådets principbeslut 3.10.2019

STRATEGI FÖR
CYBERSÄKERHETEN
I FINLAND 2019

Säkerhetskommitténs sekretariat
Södra magasinsgatan 8
PB 31, 00131 HELSINGFORS
www.turvallisuuskomitea.fi

ISBN: 978-951-663-052-9 (häft)
ISBN: 978-951-663-053-6 (pdf)

INNEHÅLL



INLEDNING

I strategin för cybersäkerheten i Finland 2019 ställs de viktigaste nationella målen upp för utvecklingen av cybermiljön och säkerställandet av de vitala funktioner som anknyter till den[1]. Syftet med strategin är också att stödja tillgången till pålitliga digitala tjänster och utvecklingen av affärsverksamheten i anslutning till dem. Strategin baserar sig på de allmänna principerna i strategin för cybersäkerheten i Finland 2013. Finlands mål är att också i fortsättningen internationellt vara bland de främsta experterna på cybersäkerhet. Förverkligandet av den nationella cybersäkerheten anknyter till Säkerhetsstrategin för samhället (2017) och till de i strategin beskrivna allmänna principerna om samordning av beredskapen och säkerheten samt om behörig myndighet. Strategin och genomförandet av den är också en del av genomförandet av EU:s cybersäkerhetsstrategi.

Behovet av att uppdatera cybersäkerhetsstrategin härleder sig från de betydande förändringar som skett i verksamhetsmiljön och från de utvecklingsområden som identifierats i den nationella verksamheten. Utvecklingen av den digitala verksamhetsmiljön tillhandahåller nya betydande möjligheter som anknyter exempelvis till plattformsekonomi, ekosystem, produktionsmodeller för nya tjänster och utveckling av terminalutrustning samt datakommunikation. Utöver de gamla riskerna, exempelvis mänskliga fel, är verksamhetsmiljön också utsatt för hot som utvecklas och förändras och som kan äventyra samhällets vitala funktioner, i synnerhet genom cyberbrottslighet, cyberspioneri, statsledd underrättelseinhämtning och olika metoder för hybridpåverkan. Flera utredningar har gjorts om det nationella cybersäkerhetsläget i Finland[2].

Förslagen i dem har beaktats i denna strategi och de beaktas också i det utvecklingsprogram som utarbetas utifrån strategin.

Genom cybersäkerhetsstrategin 2019 inleds beredningen av det nationella utvecklingsprogrammet för cybersäkerhet. Beredningen av utvecklingsprogrammet stöds av en ny samverkansmodell för ledning, där planeringen och samarbetet inom den offentliga förvaltningen och näringslivet beaktas. Programmet förbättrar lägesbilden för cybersäkerheten och kopplar tydligare samman planeringen med annan verksamhet, t.ex. den ekonomiska planeringen.

[1] Med cybersäkerhet avses ett tillstånd där man kan lita på cybermiljön och där dess funktion tryggas (Ordlista om cybersäkerhet 2018). Cybermiljön kan för sin del betraktas som samma sak som den digitala verksamhetsmiljön, som snabbt utvecklas som en del av samhället och samhällstjänsterna.

[2] I Statens tekniska forskningscentrals utredning om cyberkompetensen i Finland (2016) presenteras 12 åtgärder för att ytterligare utveckla och stärka cybersäkerhetskompetensen i Finland. I Jyväskylä universitets och Aalto-universitetets utredning om cybersäkerhetens nuläge i Finland (2017) lyfts identifierade brister i Finlands cybersäkerhet i nuläget fram liksom utvecklingspunkter kategoriserade enligt 12 delområden. Utöver dem har Statens revisionsverk offentliggjort en revisionsberättelse om organisering av cyberskyddet i Finland (2017). I berättelsen finns fem ställningstaganden och fyra rekommendationer för en utveckling av helheten. I justitieministeriets rapport Förutsättningar för internetröstning i Finland (2017) utreddes införandet av internetröstning. Arbetsgruppen rekommenderade inte att internetröstning ska tas i bruk, eftersom riskerna i dagsläget är större än nyttan. Jyväskylä universitet och Aalto-universitetet gjorde en utredning om den strategiska ledningen av cybersäkerheten i Finland (2018). I utredningen ingår förslag till åtgärder i fråga om den strategiska ledningen av samhällets och den offentliga förvaltningens cybersäkerhet, hanteringen av omfattande störningar i cybermiljön och åtgärder för att mäta cybersäkerhetsläget.

STRATEGISKA RIKTLINJER

1. UTVECKLING AV DET INTERNATIONELLA SAMARBETET – ett gränslöst tryggande av cybermiljön

Finland slår vakt om sin cybermiljö med stöd av ett aktivt internationellt samarbete och EU-samarbete.

Det internationella samarbetet är livsviktigt för Finlands cybersäkerhet. Det ligger i Finlands intresse att ha ett nära samarbete med internationella aktörer på multilateral, regional och bilateral nivå. Här avses tekniskt samarbete, politiskt samarbete och dialog.

Det internationella samarbetet stöder sig på gällande internationell rätt, internationella överenskommelser och respekt för mänskliga rättigheter också i cybermiljön. Finland vill bevara ett universellt, fritt och stabilt internet och göra en säker användning av nätet möjlig. Finland accepterar inte strävanden att begränsa friheten och öppenheten för internet och därigenom individens grundläggande fri- och rättigheter. Finland betonar rättsstatsaspekterna, demokratin och öppenheten i allt cybersäkerhetssamarbete.

Finland påverkar aktivt den internationella cybersäkerhetsagendan i Europeiska unionen och i centrala internationella organisationer (bl.a. FN, OECD, OSSE, ER, inom Nato-partnerskapet). Detta bidrar till stärkandet av det internationella regelbaserade systemet, som är ett centralt mål för Finlands utrikespolitik.

Europeiska unionens beslut samt samarbetet inom EU utgör ryggraden i Finlands nationella cybersäkerhetspolitik och utvecklingen av den. Finland deltar aktivt i utvecklingen av den gemensamma utrikes- och säkerhetspolitiken i anslutning till EU:s cybersäkerhet. EU:s reformerade cybersäkerhetsstrategi samt centrala lagstiftningsprojekt, exempelvis EU:s direktiv om nät- och informationssäkerhet (NIS), inverkar dessutom kraftigt på utvecklingen av cybersäkerheten också på det nationella planet.

Cybermiljön skyddas genom att höja tröskeln för olika slag av cyberangrepp bland annat genom förbättrande av förmågan att upptäcka och attribuera cyberangrepp och förmågan till motåtgärder. Motåtgärderna kan bestå av exempelvis brottsbekämpande åtgärder, diplomatiska åtgärder eller aktiva motåtgärder i cybermiljön. Vid utvecklandet av motåtgärder ska de riktlinjer som EU har utarbetat för ett starkt cyberförsvar beaktas. Finland deltar i bekämpningen av cyberbrottslighet genom samarbete mellan internationella rättsliga och brottsbekämpande myndigheter i EU samt genom deltagande i utvecklandet av internationell rätt och internationella överenskommelser.

2. EN BÄTTRE SAMORDNING AV LEDNINGEN OCH PLANERINGEN AV CYBERSÄKERHETEN
och beredskapen för den

Helhetsläget för den nationella cybersäkerheten förbättras genom ett utvecklingsprogram samt genom samarbete som främjar planeringen och uppföljningen av det.

Verkställighetsprogrammen för cybersäkerhetsstrategin 2013 har hittills endast grundat sig på förslag från aktörer som förbundit sig till utvecklingsarbetet och på behöriga myndigheters delvis sektorsvisa arbete. En resultatrik planering av cybersäkerheten förutsätter att de ekonomiska resurser och den samverkan som planeringen kräver beaktas med tillräcklig noggrannhet inom respektive förvaltningsområde. Detta förbättras av utvecklingsprogrammet för cybersäkerheten som sträcker sig över regeringsperioderna och som ersätter det tidigare verkställighetsprogrammet. Programmet konkretiserar de nationella riktlinjerna för cybersäkerheten och gör helhetsbilden av projekt, forskning och utvecklingsprogram som gäller cybersäkerhet tydligare.

För samordning av den nationella utvecklingen av cybersäkerheten inrättas en befattning som cybersäkerhetsdirektör vid kommunikationsministeriet. Cybersäkerhetsdirektörens roll är att samordna utvecklingen och planeringen av och beredskapen för cybersäkerheten på samhällsnivå. Inrättandet av befattningen ändrar inte på det ansvar och de befogenheter som ministerierna och de behöriga myndigheterna har i anslutning till cybersäkerhet. Cybersäkerhetsdirektören är också statsrådets rådgivare i frågor som gäller cybersäkerhet. Med utnyttjande av expertisen i ministerierna, Säkerhetskommittén och hos aktörerna inom cybersäkerhet upprättas under direktörens ledning helhetsbilden och utarbetas utvecklingsprogrammet för cybersäkerheten.

När utvecklingsprogrammet för cybersäkerhet utarbetas ska det ses till att företrädare för cybersäkerhetsindustrin, cyberforskningsinstituten och de nyckelorganisationer som svarar för viktiga tjänster inom den offentliga sektorn deltar i beredningen. Syftet med nätverksstrukturen är att intensifiera cybersäkerhetssamarbetet mellan den offentliga förvaltningen och näringslivet.

Ledningen av störningssituationer i cybermiljön och samarbetet på det operativa planet ska utvecklas mellan aktörerna inom cybersäkerhet. Vid hanteringen av störningar ska man stödja sig på en allmän hanteringsmodell för störningar och vid behov utnyttja beredskapschefsmötet.

Beredskapen för cybersäkerhet kräver samarbete mellan olika samhällsaktörer, den offentliga förvaltningen och näringslivet och stärkande av expertisen inom de olika sektorerna. De ömsesidiga beroendena inom den digitala verksamhetsmiljön kräver en helhetsarkitektur som beaktar cybersäkerheten. Fortgående verksamhet och beredskap för störningar kräver kompetens i fråga om upphandling och konkurrensutsättning, bedömning av uppfyllandet av avtalsvillkor samt övergripande kontroll över leverantörsnätet och leveranskedjorna.

Andra strategiska åtgärder för utvecklande av delområdet är följande:

- De informationsresurser, de digitala tjänster och den infrastruktur som är nödvändiga för vitala samhällsfunktioner definieras. För funktioner och servicekedjor i anslutning till dessa sätts de målnivåer upp som krävs för att hanteringen av kontinuiteten i den nationella verksamheten ska kunna säkerställas.

- Den standardenliga kravhantering som den nationella säkerheten förutsätter ska förbättras och samordnas i säkerhetskritiska tjänster. Verifiering, testning, utvärdering och användningsrekommendationer i fråga om produkter och genomförandet av hela lösningsmiljöer i anknytning till kritiska funktioner ska utvecklas så att de säkerställer att kraven uppfylls.

- I utvecklingsprogrammet vidareutvecklas myndigheternas cybersäkerhetssamarbete med tanke på den nya lagstiftningen om underrättelseinhämtning och annan lagstiftning inom det verksamhetsområdet. Centrala delområden för utvecklingen är cyberförsvaret och bekämpningen av cyberhot som äventyrar den nationella säkerheten. Vidare ska den lagstiftning som möjliggör bekämpningen av cyberbrottslighet utvecklas så att den gör effektivt förebyggande och effektiv utredning av cyberbrott möjlig.

- Cybersäkerhetscentrets förmåga att 24/7 sammanställa en lägesbild och samarbetet mellan myndigheter och näringslivet ska vidareutvecklas. Detta främjar Finlands förmåga att identifiera hot mot informationssäkerheten och varna om dem samt förbättrar näringslivets och den offentliga förvaltningens möjligheter att bereda sig för hot mot informationssäkerheten.

- Användningen och utvecklingen av digitala tjänster för säkerhetsmyndigheterna och kritiska aktörer inom näringslivet säkerställs genom särskilt skyddade lösningar som utnyttjar kommersiella tjänster och kompletterar dem i enlighet med den gällande lagstiftningen.

- Företagens produktion av kritiska tjänster i anslutning till de vitala samhällsfunktionerna och kontinuitetshanteringen ska stödas. En beskrivning av målnivån för uppgifterna och utveckling av de stödmekanismer som myndigheterna tillhandahåller gör företagens ställning tydligare. För de ansvariga myndigheterna ställs tydliga mål för utvecklingen av cybersäkerheten. Myndigheterna kan främja genomförandet av målen för cybersäkerheten bland annat genom att införa dem i kommersiella avtal och när det gäller de viktigaste frågorna behöver också lagstiftningen vid behov kompletteras.

De ömsesidiga beroendena inom den digitala verksamhetsmiljön kräver en helhetsarkitektur som beaktar cybersäkerheten.

3. UTVECKLING AV CYBERSÄKERHETS-KOMPETENSEN – vardagliga färdigheter och experter som garanter för cybersäkerheten

Den nationella kompetensen inom cybersäkerhet säkerställs genom identifiering av kompetensbehovet och genom stärkande av utbildningen och forskningen.

Det finländska samhället behöver kompetens inom cybersäkerhet, både i den offentliga förvaltningen och i näringslivet. Den nationella cybersäkerheten byggs upp som ett samarbete mellan myndigheter, näringslivet och medborgarna och alla kan själv påverka vår gemensamma cybersäkerhet. Varje individ är alltså en viktig cybersäkerhetsaktör som genom sina vardagliga handlingar för att förbättra cybersäkerheten kan påverka både sin egen och andras cybersäkerhet. Nationellt ska det säkerställas att alla har tillräckliga färdigheter för att agera på ett tryggt sätt i den digitala verksamhetsmiljön.

Myndigheterna och företagen behöver synnerligen mångsidig kompetens, både bland anställda och bland underleverantörer, för att kontrollera riskerna i anslutning till cybersäkerhet. På nationell nivå ska det ses till att företagen har tillräckligt med personal med spetskompetens och annan kunnig personal. Kompetensutvecklingen framhävs också i samarbetet mellan näringslivet och forskningen. Genom intensivt samarbete, informationsutbyte om kundbehov och genom att förbättra tjänsteutvecklingen kan man skapa betydande ny kompetens på den nationella inre marknaden.

Med tanke på kompetensfrågan och konkurrenskraften är det viktigt att hitta nya metoder genom vilka de nationella företagen kan behålla sina anställda med spetskompetens då den internationella konkurrensen ökar. Med tanke på Finlands konkurrenskraft är det också väsentligt att de internationella säkerhetsstandarderna stöder produkter där finländska företag är starka inom tillverkningen. Det är viktigt att fortsätta med det aktiva deltagandet i standardiseringsarbetet och tillverka produkter med inbyggd säkerhet. På så sätt kan man samtidigt förbättra möjligheterna för våra nationella företag som är specialiserade inom de områdena att nå framgång i den internationella konkurrensen.

Med tanke på samhällets cybersäkerhet och näringslivet är det en central fråga hur man får cybersäkerheten att bli en viktig del av verksamheten även hos andra företag än de företag som producerar produkter, tjänster och lösningar inom cybersäkerhet. Företag med egentlig affärsverksamhet utanför cybersäkerhetssektorn men på vars verksamhet cybersäkerheten med anknytande störningar

Den nationella cybersäkerheten byggs upp som ett samarbete mellan myndigheter, näringslivet och medborgarna och alla kan själv påverka vår gemensamma cybersäkerhet.

har en betydande inverkan spelar en allt större roll i framtiden. Sådana branscher har beskrivits i synnerhet i lagstiftningsprojekt som gäller nät- och informationssäkerhet, och i dessa har som sådana branscher betraktats bland andra datakommunikation, energiproduktion och energidistribution, försäkringsbranschen och hälso- och sjukvård.

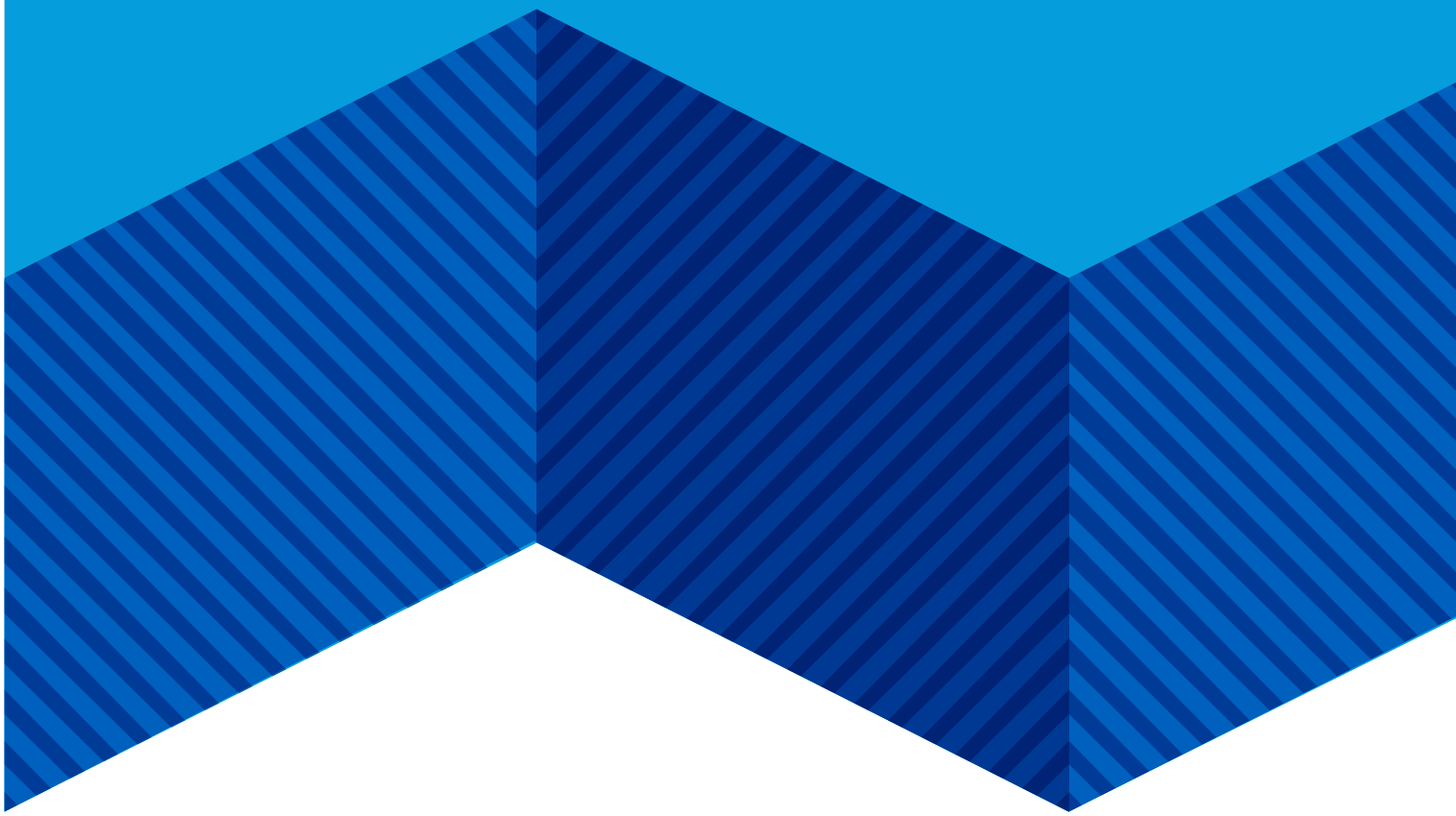
Utvecklingen av cybersäkerheten ställer krav på kompetens och medför samarbetsförpliktelser för den offentliga förvaltningen. Hos myndigheter med ansvar för kritiska funktioner ska ansvaret för styrning, stöd och övervakning i fråga om cybersäkerhet och de resurser och den arsenal av metoder detta kräver förbättras inom alla förvaltningsområden och på alla nivåer.

Andra strategiska åtgärder för att främja cybersäkerhetskompetensen är följande:

- Utbildningsprogrammen i anslutning till cyber- och informationssäkerhet, utvecklingen av programvaror och applikationer samt i anslutning till informationsnät och datakommunikation stärks i yrkesutbildningen och vid yrkeshögskolor och universitet.
- Den utbildning på hög nivå som krävs för de nationellt kritiska cyberkompetensområdena säkerställs. Detta stöds både genom nationell och internationell utbildning och genom övningsverksamhet.
- Den nationella forsknings-, utvecklings- och testningsverksamheten för cybersäkerhet stärks.
- Det riksomfattande utbildnings- och övningssystemet för digital säkerhet stärks som en del av den offentliga förvaltningens utbildning inom digital säkerhet. På så sätt utvecklas kompetensen hos de anställda i den offentliga förvaltningen, företagen och andra intressentgrupper samt hos medborgarna.
- Medvetenheten om informationssäkerheten för nya tjänster och produkter inom den offentliga förvaltningen, i näringslivet och hos enskilda människor höjs. Cybersäkerhet är ett ovillkorligt krav för dataekonomin och applikationer som baserar sig på artificiell intelligens. Det kräver att tillverkarna och tjänstetillhandahållarna litar på varandra och att medborgarna litar på de tjänster och produkter som de erbjuds.

STRATEGIN FÖR CYBERSÄKERHETEN I FINLAND

www.turvallisuuskomitea.fi



Turvallisuuskomitea
Säkerhetskommittén
The Security Committee