Se upp för de fula fiskarna

Finlands väg till ökad cybersäkerhet

Theo Herold

AGENDA

Tankesmedjan Agenda 2024
ISBN 978-952-7273-48-7 (tryckt)
ISBN 978-952-7273-49-4 (pdf)
Grafisk layout och ombrytning: Linnéa Sjöholm
Illustrationer: Sebastian Dahlström
Kommentarens översättning: Anu Huusko / TranslatiOm Finland

Se upp för de fula fiskarna

Finlands väg till ökad cybersäkerhet

Tankesmedjan Agenda
Theo Herold
2024

Innehållsförteckning

Om skribenten

Foto: Tom Samuelsson

Theo Herold doktorerar i nationalekonomi vid Hanken och Helsinki Graduate School of Economics. Han är associerad forskare vid forskningsinstitutet Ratio i Stockholm och redaktör för forskningsdelen av tidskriften Liberal Debatt. Han har tidigare jobbat för Stockholms Handelskammare med frågor som delvis berör cybersäkerhet och -beredskap.

Förord

Det är helt okej att bli lurad på nätet – du är inte ensam

Foto: Anders Wikström

Jag har blivit snuvad på pengar över nätet två gånger. Det var inte stora summor, men jag kände mig extremt dum, förödmjukad och lurad efteråt. Efter den första gången lovade jag mig att det aldrig skulle ske igen. Efter den andra gången såg jag mönstret. En tredje gång har det inte skett.

I rubrikerna ser vi regelbundet ord som datastöld, lösenordsfiske och nätbedrägerier. Men också gps-störningar, överbelastningsattacker och hybridkrigföring. Cyberbrottsligheten från både ensamt agerande aktörer, kriminella nätverk och från statsmakter – ibland en kombination av alla tre – är tyvärr här för att stanna.

Alltefter att våra liv flyttat ut på nätet så har brottsligheten följt efter. Man brukar säga att tillfället gör tjuven, och på nätet finns det gott om både tillfällen och tjuvar. Man brukar även säga att det gäller att se om sitt hus. Då det gäller den fysiska världen så vet vi att man ska regla ytterdörren, låsa fast cykeln och inte lämna plånboken efter sig på kafébordet.

Men då det kommer till det digitala är det knepigare. Det digitala är i konstant förändring då ny teknik och nya möjligheter ständigt dyker upp. Det viktiga är att vara förbered.

Därför publicerar Agenda nu en rapport om ämnet. Nationalekonomen Theo Herold (Svenska Handelshögskolan) ger en inblick i vad cyberbrottslighet är och hur mycket det kostar Finland (svaret är mycket!), vad som görs för att förbättra cybersäkerheten (både för nation och individ) samt vad vi kunde lära oss av Estland, som ligger steget före i mångt och mycket som gäller den digitala sfären.

Rapporten presenterar även konkreta åtgärder för förbättrad cybersäkerhet samt en kommentar av Försörjningsberedskapscentralen om hur individen och staten kan stärka cybersäkerheten.

Det räcker inte bara med tvåstegsverifiering och stark autentisering. Det gäller också att känna igen när någon vill åt dina data, lösenord eller din identitet genom att vara i direkt kontakt.

Helsingfors, november 2024

Ted Urho
Verksamhetsledare
Tankesmedjan Agenda

1. I en värld uppkopplad mot cyberdomänen

Samhället lever i dag på många sätt över internet, i cyberdomänen. Cyberdomänen innefattar kommunikationsförbindelser som utförs med hjälp av elektroniska enheter såsom datorer, pekplattor och mobiler, men också enheter såsom övervakningskameror och inspelningsapparater. Privatpersoner gör betalningar med digitala plånböcker, myndighetsärenden sköts i digitala brevlådor och resenärer använder sig av mobila buss- och transportkort. Samhällsinfrastrukturen i stort kräver helt eller delvis uppkoppling till cyberdomänen, från elen i elnätet, till trafikljusen kring våra vägar och transportsystemen över Östersjön.

I takt med att samhällen uppkopplas mot internet så ökar också frekvensen av cyberbrott. Cyberbrottslighet innefattar sådan olaglig verksamhet där en förövare med hjälp av och över elektroniska enheter begår brott. Brotten kan innefatta allt från olaga åtkomst till känslig information, utpressning, att sprida rädsla och desinformation, samt störa viktiga samhällsfunktioner. Förövare kan agera ensamma eller som del av större nätverk och ett allt vanligare inslag är statsmakters inblandning i sådan verksamhet. Cyberangrepp kan riktas mot enskilda individer, grupper och hela samhällen. Därför är det viktigt att garantera cybersäkerheten hos den enskilda individen, upp till myndigheter och större institutioner.

Att kommunikationsinfrastrukturen och cybersäkerheten håller hög kvalitet är helt centralt för att det moderna samhället ska fungera. För Finlands del ökar vårt geografiska läge bredvid Ryssland behovet av en god cybersäkerhet. Ryssland har en lång historia inom cyberbrottslighet och utgör det enskilt största säkerhetspolitiska hotet mot Europa. Ryska cyberbrottsligor, som till exempel Avalanche och NoName, har över åren riktat flera större angrepp mot privatpersoner, företag och myndigheter i Finland. Det är högst troligt att dessa ligor ofta agerar på bevåg av den ryska staten.

Ett stort hinder för att öka cybersäkerheten i samhället är att den digitala utvecklingen är snabb och därmed ändrar sig också cyberattackernas natur över tid. Och för varje typ av angrepp som vi lyckas gardera oss mot, verkar det växa fram tiotals nya typer av angreppssätt. Går det ens att skydda sig helt? Det krassa svaret är nej, inte egentligen, men det är också en sanning med modifikation.

Genom en samhällsgemensam samverkan kan vi minimera skadans storlek och risken att bli utsatta. Som privatpersoner bör vi hålla oss själva underrättade och öka vår förståelse för hur olika typer av cyberangrepp fungerar. Beslutsfattare på kommunal och statlig nivå måste se till att dialogen mellan myndigheterna och näringslivet fungerar smärtfritt. Både det privata och offentliga måste möjliggöra nödvändiga investeringar i kommunikationsinfrastrukturen. Mellan stat – företag – individ måste informationsutbytet löpa fritt och en tydlig ansvarsfördelning göras.

I kölvattnet av Finlands Natomedlemskap är det också viktigt att vi ökar vår samverkan med resten av Norden och Europa. Det finns mycket inspiration att hämta från våra grannländer i Baltikum och kanske särskilt från Estland. Estland har en världsledande roll inom både cybersäkerhet och digitalisering, vilket är resultatet av utbildningsmöjligheter redan i ett tidigt skede, en stark samverkan mellan det offentliga och privata, samt (tyvärr) också utifrån landets omfattande erfarenhet av cyberangrepp.

Det hänsynslösa anfallskriget mot Ukraina vittnar också om hur en stat, i detta fall Ryssland, kan involvera sig i cyberbrottslighet. Dagen före invasionen, den 22 februari år 2022, utfördes angrepp mot banker och myndigheter i form av överbelastningsattacker och spridandet av skadlig kod. Mycket tyder på att koden redan utvecklats under år 2021, vilket skulle kunna innebära att attacken var planerad flera år i förväg.[1] Under perioden före invasionen utförde Ryssland en rad liknande attacker mot myndighetssidor som drabbade bland annat det ukrainska regeringskansliet och utrikesdepartementet. Somliga kommer kanske ihåg rapporteringen om texten ”var rädda och förbered er för det värsta” som spreds på ukrainska myndighetssidor.[2] Under krigets gång har Ryssland fortsatt sin hybridkrigföring.

För Finlands del har Ryssland genom åren riktat flera överbelastningsattacker, även kallade DDoS-attacker, mot bland annat Skatteförvaltningen, Traficom, Expressbus, riksdagen och flera andra myndigheter. Under år 2024 har flera gps-störningar stört trafiken runt Östersjön både i luften och till havs, och av allt att döma är det Ryssland som ligger bakom dessa angrepp.[3]

1 ESET Research, ”IsaacWiper and HermeticWizard: New wiper and worm targeting Ukraine”, We Live Security, 2022.

2 Andrew Kramer/The New York Times, ”Hackers Bring Down Government Sites in Ukraine”, 2022.

3 Dann Pettersson/Hufvudstadsbladet, ”Finnair pausar flyg efter gps-störningar”, 2024.

Cyberbrottsligheten från både ensamt agerande aktörer, kriminella nätverk och från statsmakter – ibland en kombination av alla tre – är tyvärr här för att stanna.

Du håller i en rapport vars syfte är att öka den generella förståelsen för cyberbrottsligheten, i vilka former den kommer och hur vi i det finländska samhället ökar vår motståndskraft mot den. För att göra detta återges först en kort historisk tillbakablick och kostnadsestimat över cyberbrottsligheten (kapitel 2). Därefter diskuteras hur cybersäkerheten utvecklats i Finland och hur den fungerar i dag (kapitel 3). Vi tittar sedan närmare på den estniska excellens som lett till att Estland blivit världsledande inom både digitalisering och cybersäkerhet, och vad vi i Finland kan lära oss av vår Östersjögranne (kapitel 4). Rapporten avslutas med att återge konkreta förslag på hur Finland kan utveckla sin cybersäkerhet (kapitel 5).

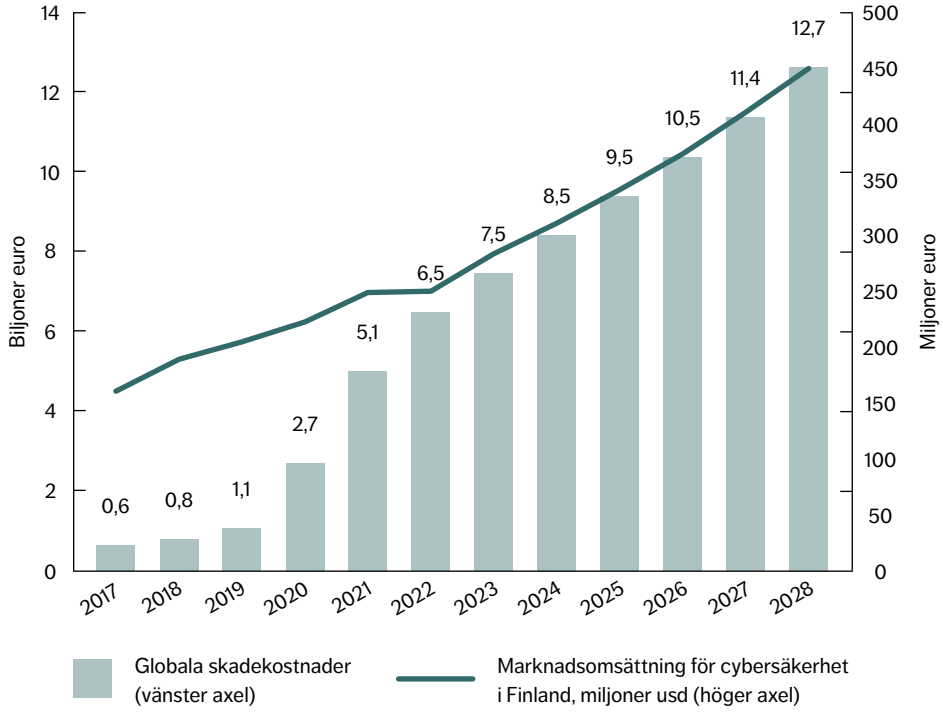
2. Cyberbrott – kostnader i miljoner för finska staten

Det var i samband med den snabba digitala utvecklingen och utbredningen av privatdatorn under 1990-talet som cyberbrottsligheten på riktigt tog fart. Det är svårt att retroaktivt estimera hurudana pengasummor som angripare under den här tiden kunde tjäna, för att inte prata om storleken på skadekostnaderna som de förorsakade. Vad vi dock kan konstatera, och som framkommer i figur 1, är att den globala cyberbrottslighetens skadekostnader i dag är alldeles astronomiska. År 2028 förväntas de uppgå till 12,7 biljoner (biljoner med ett b!) euro – för att belysa hur absurd denna summa är så skriver vi ut den: 12 700 000 000 000 euro. Om cyberbrottsligheten var ett land skulle den utgöra världens tredje största ekonomi efter USA och Kina.[4] För referens uppgick Finlands bnp, värdet på den ekonomiska aktiviteten i Finland, till cirka 280 miljarder euro år 2022 – alltså ”bara” 280 000 000 000 euro. Cyberbrottslighetens skadekostnader under ett givet år överstiger de ekonomiska kostnaderna som världens alla naturkatastrofer tillsammans förorsakar, eller den direkta kostnaden för hela den globala droghandeln.[5] Till följd har marknaden för olika cybersäkerhetslösningar också vuxit så det knakar – som framkommer i figur 1 förväntas marknadsintäkterna i Finland öka med 180 procent upp till 450 miljoner euro mellan år 2017 och år 2028.

4 Europeiska kommissionen estimerade att de globala skadekostnaderna för cyberbrott redan år 2020 uppgick till 5,5 biljoner euro, alltså något högre än estimatet i figur 1. Se Europeiska kommissionen, ”A cybersecure digital transformation in a complex threat environment, 2019. Steve Morgan/Cybercrime Magazine, ”Cybercrime to cost the world $10.5 trillion annually by 2025”, 2020.

5 Mai Periman/Cisco, ”How to prevent the bank robbery no one can see”, 2017.

FIGUR 1 Cyberbrottslighetens skadekostnader globalt och marknadsintäkterna för cybersäkerhet i Finland, 2017–2028



Not: Notera att vänster axel som visar skadekostnaderna är biljoner euro, medan höger axel som visar marknadsomsättningen för cybersäkerhet i Finland är miljoner euro. Källa: Statista Technology Market Insights

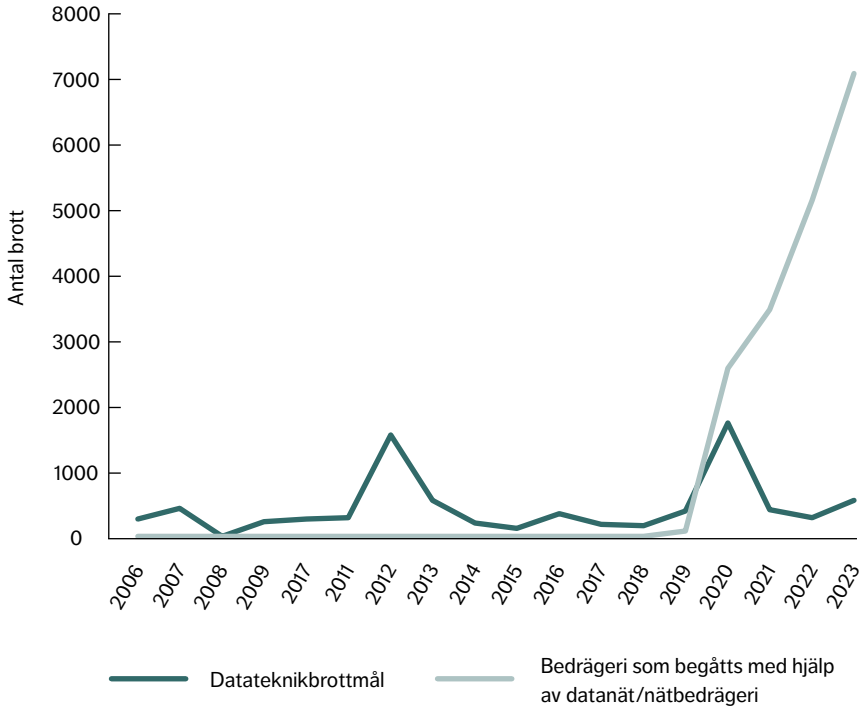
Mot privatpersoner är datastöld och bedrägerier vanligast och de utförs ofta med hjälp av lösenordsfiske. Det är inte konstigt med tanke på hur aktivt vi i Finland använder internet – år 2023 uppgav 94 procent att de använt internet åtminstone en gång under de tre senaste månaderna, medan 73 procent använder internet flera gånger om dagen.[6] Att vi flitigt använder internet märks tyvärr också i frekvensen av internetbedrägerier, då över 7 000 sådana brott kommit till polisens kännedom under år 2023; se figur 2.[7] Sedan 2019 har antalet

6 Statistikcentralen, ”Befolkningens användning av informations- och kommunikationsteknik”.

7 Finanssiala Ry, ”Varo, varmista ja varoita: Nettihuijaukset ja tietojenkalastelu muuttavat muotoaan, mutta niiltä on mahdollista suojautua”, 2022.

internetbedrägerier ökat explosionsartat och allting tyder på att detta kommer hålla i sig. För år 2023 estimeras det att finländare lurats på över 40 miljoner euro.[8] Även olika typer av kärleksbedrägerier blir allt vanligare. Artificiell intelligens gör det lättare att imitera text, röst och bild, ofta av någon person som står offret nära, vilket också ökar sannolikheten att falla offer för lösenordsfiske och andra bedrägerier.[9]

FIGUR 2 Datateknikbrottmål och bedrägerier på nätet som kommit till polisens kännedom, 2006–2023



Källa: Polisen, Statistikcentralen

8 Markku Korhonen/Cryptonews, ”Valtavaa kasvua: Digihuijaukset Suomessa lisääntyivät”, 2024.

9 Niklas Fagerström/Yle, ”Finländare har lurats på rekordmycket pengar på nätet – det handlar om tiotals miljoner euro på ett halvår”, 2023.

Så vad kostar cyberbrottsligheten egentligen? För att uppskatta detta tar vi först fram mängden dataskadegörelse, dataintrång och dataskyddsbrott som polisen fått kännedom om som berör myndigheter, företag och privatpersoner. Det är viktigt att komma ihåg att databrott inte är skapta lika – skadekostnaderna kan variera kraftigt från fall till fall. Det är också viktigt att påpeka att det antagligen finns ett stort mörkertal, där företag och individer inte vågar, vill eller kan polisanmäla angreppet. Det totala antalet fall av dataintrång, dataskadegörelse och dataskyddsbrott som kommit till polisens kännedom uppgick till cirka 17 000 under år 2023. Antalet grova dataintrång har ökat explosionsartat mellan år 2022 och år 2023, vilket troligtvis beror på en kombination av att angreppen faktiskt blivit mer frekventa, att attackytan per företag blivit större och att vissa fall som begåtts tidigare kommit till polisens kännedom under år 2023.[10] En särskild aspekt är att dataintrång som sprider sig till många applikationer klassificeras som flera olika brott, vilket gör att siffran är högre än om samma angrepp klassificeras som ett angrepp oberoende hur många applikationer som berörs. Därför tar vi fram ett lågscenario där vi antar att unika grova dataintrång är en femtedel av vad som de facto kommit till polisens kännedom. I lågscenariot är det totala antalet fall cirka 4 300.

Om vi utgår ifrån kostnaderna för internetbedrägerier i Finland och den genomsnittliga kostnader per cyberangrepp mot företag och myndigheter i Europa, som mellan perioden 2021 och 2023 var cirka 14 000 euro, så skulle de totala kostnaderna för cyberbrottslighet uppgå till nästan 290 miljoner euro under år 2023.[11] Det utgör ungefär 7 procent av samtliga anslag i statens budget för år 2024. Det är mer än vad som anslås till Utrikes-, Justitie-, Inrikes- och Försvarsministeriet – tillsammans! I jämförelse med andra länder som till exempel Sverige är den uppskattade kostnaden förhållandevis låg – enbart kostnaden av cyberangrepp mot svenska företag uppgick till cirka 2 miljarder euro redan år 2021.[12] På grund av de redan nämnda mörkertalen är det alltså inte omöjligt att kostnaderna i Finland är högre än vad som rapporteras i tabell 1. Kostnaden är hur som helst en bromskloss för Finlands konkurrenskraft och företagens tillväxt.

10 I korrespondens med Statistikcentralen, som tillhandahåller brottsstatistik från Polisen, är det just dessa faktorer som förklarar den enorma ökningen i specifikt grova dataintrång från år 2022 till år 2023.

11 Denna genomsnittliga kostnad för cyberbrott är tagen från Statista Market Insight och kommer från Hiscox och Forrester Research.

12 Stockholms Handelskammare, ”Cyberbrott mot svenska företag – hur bygger vi en säkrare framtid?”, 2022.

TABELL 1 Skadekostnadsestimat för finska staten av samtliga cyberangrepp, 2023

Beskrivningspost	Estimat
Till polisens kännedom inkomna fall	
Dataskadegörelse, antal	80
Dataintrång, antal	2 097
Grovt dataintrång, antal	14 171
Dataskyddsbrott, antal	697
Totala fall, antal	**17 045**
Totala fall i lågscenario för grovt dataintrång, antal	**4 291**
Övriga variabler	
Kostnadsgenomsnitt per attack i Europa, 2021–2023	14 636 €
Kostnaden för bedrägerier i Finland, 2023	40 000 000 €
Totala kostnader, 2023	**289 470 620 €**
Totala kostnader i lågscenario, 2023	**102 804 540 €**

Källa: Statistikcentralen, Polisen, Statista, Markku Korhonen/Cryptonews

3. Arbetet med cyber-säkerhet i Finland

Hotet från en annan statsmakt, särskilt Ryssland, är mer aktuellt än någonsin. Som vi konstaterat inledningsvis måste cybersäkerheten hålla hög kvalitet för att det moderna samhället ska fungera. Detta ansvar har också nu utökats ytterligare, som en del av Finlands Natomedlemskap. Finland har tagit viktiga steg under de senaste åren.

I Finland hjälper säkerhetskommittén både Statsrådet och ministerierna i ärenden som berör övergripande säkerhet. Säkerhetskommittén består av en ordförande, vilket i praktiken är kanslichefen för Försvarsministeriet, samt kanslichefer från ministerierna, polisöverdirektören, Tullens generaldirektör, och så vidare. Till säkerhetskommitténs uppgifter hör samordningsarbete för att säkra samhällets vitala funktioner, upprätthålla försörjningsberedskapen och garantera en god framförhållning. Trots att säkerhetskommitténs ansvar ligger utanför den direkta cybersäkerheten så är dess arbete direkt knutet till cybersäkerheten.

År 2013 lanserade säkerhetskommittén Finlands första cybersäkerhetsstrategi. Strategin fastställde ansvarsfördelningen för cybersäkerheten genom att statsrådet står överst, men att varje ministerium ”svarar för cybersäkerheten och för hanteringen av de störningssituationer som anknyter till den”.[13] Detta kom delvis att revideras med den nya cybersäkerhetsstrategin från år 2019 (och som fortfarande gäller i dag). Bland annat inrättades befattningen cybersäkerhetsdirektör vid Kommunikationsministeriet med uppgiften ”att samordna utvecklingen och planeringen av och beredskapen för cybersäkerheten på samhällsnivå.”[14] Strategin påpekade dock att inrättandet av den nya befattningen inte ändrar ”på det ansvar och de befogenheter som ministerierna och de behöriga myndigheterna har i anslutning till cybersäkerhet.”[15] Statens cybersäkerhetsdirektör i dag är Rauli Paananen.

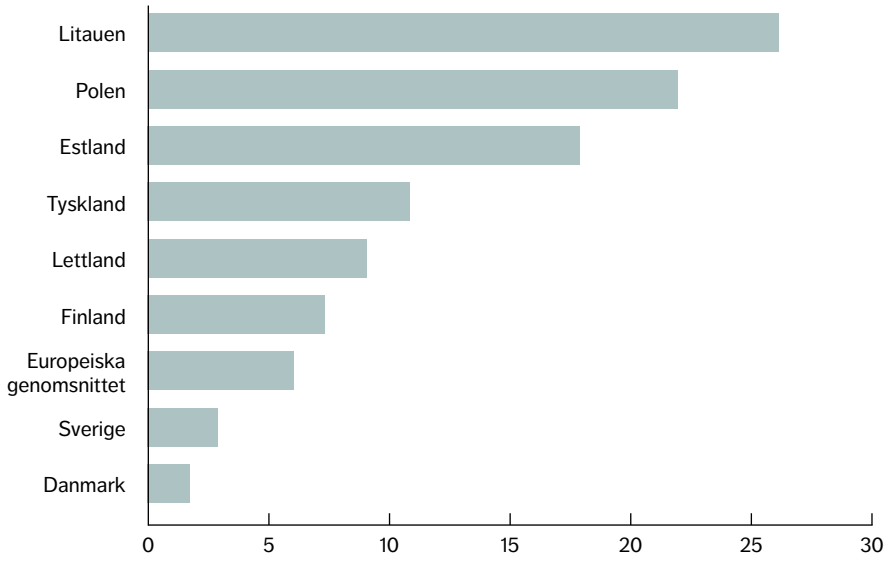
13 Säkerhetskommittén, ”Strategi för cybersäkerheten i Finland”, 2013.

14 Säkerhetskommittén, ”Strategi för cybersäkerheten i Finland 2019”, 2019.

15 Ibid.

En av de ledande målsättningarna i den första cybersäkerhetsstrategin var att Finland redan år 2016 skulle vara en global föregångare inom beredskapen inför cyberhot. Med facit på hand kan vi säga att vi inte nådde ända fram. e-Governance Academy tar fram ett National Cybersecurity Index och ett Digital Development Index som subtraheras med varandra för att mäta hur väl ett lands cybersäkerhet matchar behovet som landets digitala utvecklingsgrad ställer. Detta framställs i figur 3. Talen ska ses som relativa i bemärkelsen att ett land med ett högre nettotal bättre tillfredsställer de cybersäkerhetsbehov som finns i landet. I vår direkta närhet presterar Baltikum, Polen och Tyskland bättre än Finland. Finland kan se det positiva att vi placerar oss strax ovanför EU-genomsnittet, men det är knappast ett värdigt resultat för ett land med målsättningen att vara föregångare inom cyberberedskapen. Det går inte att vara världsledande inom teknologi och it-infrastruktur utan att också vara världsledande inom cybersäkerhet och cyberberedskap.

FIGUR 3 Nettotal över hur väl cybersäkerheten tillfredsställer det befintliga behovet

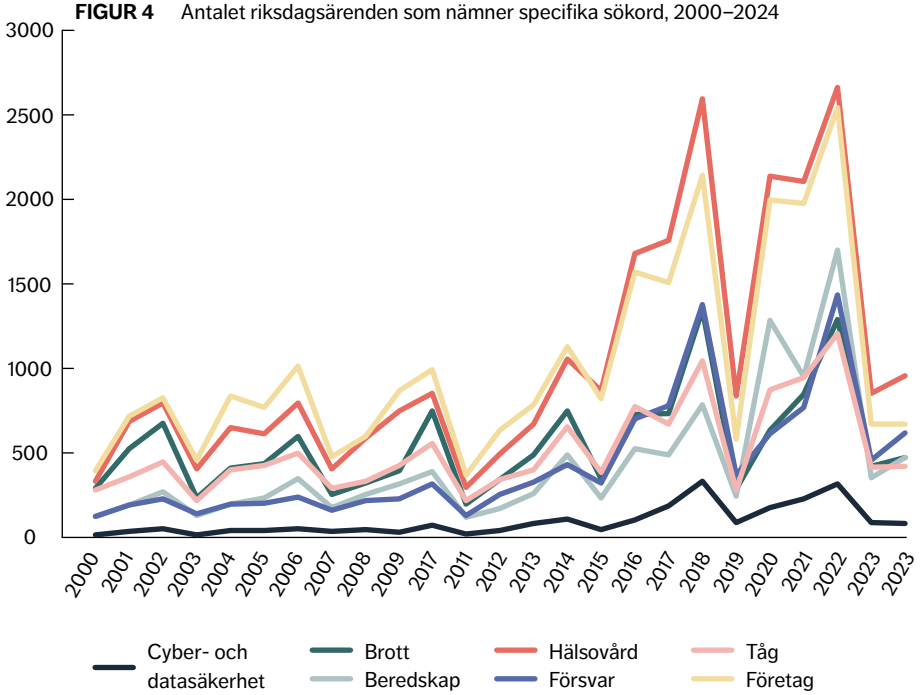


Not: Bygger på en sammanvägd bedömning av den lagstiftning, de policybeslut och den samverkan som finns mellan berörda aktörer i samhället. Ett tal lika med noll innebär att minimikravet på cybersäkerhet uppfylls, givet den befintliga digitala infrastrukturen. I sammanhanget ska det påpekas att ett nettotal kan vara högt trots att cybersäkerheten i absoluta termer är lägre, vilket är fallet om den generella digitala utvecklingen är låg.
Källa: e-Governance Academy

Specifikt frågan om cybersäkerhet har fått förhållandevis lite uppmärksamhet av landets politiker. I figur 4 framställs frekvensen av olika begrepp som vi sökt på Riksdagens hemsida – från ”cybersäkerhet” till ”tåg”, ”företag” och ”hälsovård”. Figuren sammanställer alltså hur många dokument som associeras med sökordet över tid, från år 2000 fram till år 2024. De återkommande hacken som går att se beror på att regeringar i slutet av mandatperioden skruvar upp sin aktivitetsgrad, medan det för nytillträdda regeringar tar en stund att komma i gång. För ”cyber- och datasäkerhet” har jag gjort två skilda sökningar, en för ”cybersäkerhet” och en för ”datasäkerhet” som jag sedan summerat.

Cyber- och datasäkerhet verkar inte prioriteras lika högt som de andra områdena. Den högsta siffran för cyber- och datasäkerhet noterades år 2022 när antalet riksdagsärenden uppgick till 314. Jämförelsevis översteg antalet dokument för samtliga övriga begrepp 1 000 under samma år. Trenden framöver är heller inte starkt uppåtgående. Sedan år 2023, efter regeringen Marin, har skillnaden gentemot övriga begrepp blivit betydligt mindre, men då ska det också kommas ihåg att år 2024 är regeringen Orpos andra år vid makten. På basis av den historiska trenden kommer denna skillnad mellan cyber- och datasäkerhet gentemot de övriga begreppen högst troligen att växa ju längre mandatperioden hinner löpa.

FIGUR 4 Antalet riksdagsärenden som nämner specifika sökord, 2000–2024



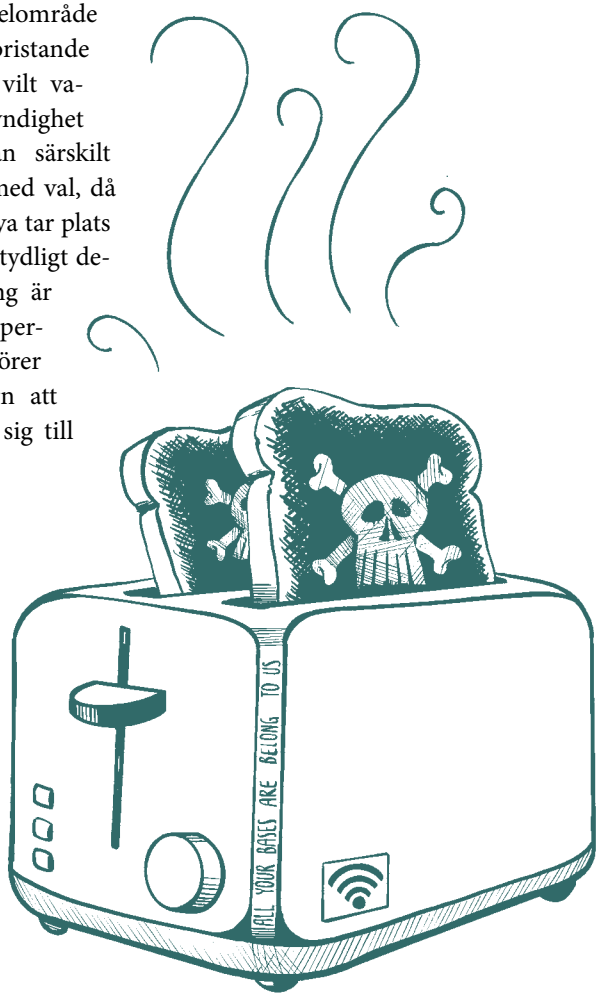
Not: Samtliga begrepp söktes 9.30.2024 på Riksdagens webbsida. Källa: Finlands riksdag

På Riksdagens webbsida går det dessutom att se hur stor andel av de olika sökorden som också associeras med andra så kallade ”ämnesord”. Om vi till exempel söker på ”Beredskap” så går det att få fram hur många av dessa dokument som också associeras med ”cybersäkerhet”. Dokument som också associeras med cybersäkerhet är 0,1 procent för ”företag”, 0,13 procent för ”brott”, 0,38 procent för ”beredskap” och 0,42 procent för ”försvar”. Den låga andelen kan te sig konstig, särskilt eftersom detta är områden där cybersäkerheten upplevs som viktig eller tätt sammankopplad. Allt fler företag uppger att deras största utmaningar består av störningar i värdekedjorna och cyberangrepp.[16] Därutöver utgör cyber- och datasäkerheten en alldeles central del av bekämpningen av brott och går naturligt ihop med en förbättrad beredskap och ett förstärkt försvar.

I närtiden har beslutsfattare dock skickat flera goda signaler om ökade ambitioner på cybersäkerhetsområdet. År 2022 framarbetades den digitala kompassen för Finland år 2030 som också inkluderar cybersäkerhetens målsättningar på ett hörn. En av de nämnvärda målsättningarna är att öka personers generella kompetens kring digitala verktyg och cybersäkerhet. År 2023 lanserades en av Inrikes- och Försvarsministeriet framtagen rapport med åtgärder som kan utföras på kort och lång sikt.[17] En långsiktig åtgärd är bland annat möjligheten för Försvarsmakten, Polisen, Skyddspolisen och Traficom att lättare kunna dela och analysera viss information sinsemellan. Av de kortsiktiga åtgärderna efterlyses bland annat en uppdatering av rådande cybersäkerhetsstrategi och förbättrad samverkan mellan offentliga och privata aktörer. Utredningen har delvis burit frukt, då Statsrådets kansli den 8 mars 2024 tillsatte en utredning för att utveckla verksamhetsmodellen för Statsrådets säkerhetsledning, vilket också inkluderar en reform av Finlands cybersäkerhetsstrategi. Reformarbetet med cybersäkerhetsstrategin förbereds av en undergrupp som leds av statens cybersäkerhetsdirektör. Arbetsgruppens mandattid löper fram till den 31 oktober år 2024.

Det finns en rad olika samverkansytor i dag, bland annat genom Traficoms cybersäkerhetscenter, vars syfte är att sammanföra aktörer från den offentliga, privata och tredje sektorn.[18] Centret har också i uppgift att hjälpa aktörer med monitorering och incidenthantering, lägesbedömningar och rådgivning. Under 2023 började även Finlands nationella samordningscentrum (NCC-FI) bedriva sin verksamhet inom ramen för cybersäkerhetscentrets forsknings-, utvecklings- och innovationsverksamhet. Som nämndes inledningsvis så hänger cybersäkerhet, transportinfrastruktur och försörjningsberedskap tätt ihop, vilket innebär att även Försörjningsberedskapscentralen är en relevant aktör i cybersäkerhetens bemärkelse. Försörjningsberedskapscentralen, som ligger under Statsrådet, har delvis i uppgift att sammanföra relevanta aktörer inom försörjningsberedskapen.

Medan vissa åtgärder, som till exempel inrättandet av statens cybersäkerhetsdirektör, vittnar om en välmenad vilja att öka cybersäkerheten i samhället, så löper den stora mängden institutioner risken att göra ansvarsfördelningen diffus. Att varje enskild myndighet bär ett stort ansvar för sitt delområde kan också leda till ett bristande informationsutbyte och vilt varierande praxis från myndighet till myndighet. Det kan särskilt accentueras i samband med val, då tjänstemän byts ut och nya tar plats i ministerierna. Utan en tydligt definierad ansvarsfördelning är det också svårt för privatpersoner, företag och aktörer inom den tredje sektorn att veta vem de bör vända sig till vid cyberangrepp.



16 Allianz, ”Risk Barometer – Identifying the major business risks for 2023”, 2022.

17 Statsrådet, ”Utredning: Finlands cybersäkerhet bör utvecklas målmedvetet och myndigheternas samarbete och processer förbättras ytterligare”, 2023.

18 Traficom Cybersäkerhetscentret, ”Nationella samordningscentrumets uppgifter”, 2023.

4. Den estniska excellensen

Sedan frigörelsen från Sovjetunionen år 1991 har Estland gjort stora digitaliseringssatsningar. Redan år 1994 antog Estlands parlament ett principprogram, där en av målsättningarna var att öronmärka en procent av bnp för investeringar i informationsteknologi. År 1996 lanserades de första e-banktjänsterna och över tid har så gott som alla offentliga tjänster gjorts digitala och förts över till vad som kallas för ”e-Estonia”. Enligt det så kallade e-Estonia Briefing Centre är 99 procent av landets samtliga offentliga tjänster tillgängliga online 24 timmar om dygnet, 7 dagar i veckan. e-Estonia innefattar bland annat en nationell parkeringstjänst, möjligheten att registrera äktenskap digitalt, streaming av politikersammanträden, och mycket mer. Informationsflöden över e-Estonia omfattas av avancerad kryptering och digitala signaturer.

Estland etablerade världens första dataambassad i Luxemburg år 2015. Syftet med dataambassaden är att skydda och upprätthålla hemligstämplad information och tillhandahålla backupenheter av kritiska dataflöden. Större dataset som lagras i dataambassaden inkluderar domstolarnas filsystem, landregistret, individuell skatteinformation, populationsregistret, och så vidare. Ambassaden har ett så kallat ”Tier-4” säkerhetsskydd, vilket är den högsta nivån av säkerhet för större datacenter. Ambassaden och dess medarbetare har diplomatisk immunitet och enheten drivs av Estlands utrikesministerium.

Parallellt med en hög digitaliseringsgrad har Estland likaså en hög nivå på landets cybersäkerhet. Trots det skulle det räcka fram till år 2007 innan Estland gav lika hög prioritet till cybersäkerheten.

Överbelastningsattackerna riktade mot Estland år 2007 utgör än i dag en av de största överbelastningsattackerna hittills. De följde i kölvattnet av en lång dispyt mellan Estland och Ryssland, efter att estniska beslutsfattare kommit överens om att flytta den sovjetiska ”Bronssoldaten” bort från Tallinn. Överbelastningsattacker har som syfte att rikta internettrafik för att på så vis överbelasta en webbsida, vilket också leder till att ingen annan har tillgång till webbsidan. Attackerna gör det svårt att ta del av tjänster och information. Attackerna riktades mot banker, massmedia och myndigheter. De angripna bankernas onlinetjänster låg nere, mediehus hade svårt att förmedla nyheter och myndigheters

kommunikationsförbindelser slogs ut. Attackerna höll på i tre veckor och olika ryska grupperingar har tagit ansvar för attackerna. Mycket tyder på att attackerna skett i nära samverkan med ryska myndigheter.

Nato inledde en stor undersökning för att kartlägga händelseförloppet och etablerade år 2008 Natoenheten ”NATO Cooperative Cyber Defence Centre of Excellence”, även kallat CCDCOE, i Tallinn. CCDCOE arbetade snabbt fram den så kallade Tallinnmanualen om hur internationell rätt gäller i frågor som berör cyberkonflikter. I dag är CCDCOE en central aktör inom försvarsalliansens arbete med cyberförsvar och är en plattform för att utveckla gemensam praxis, bedriva forskning och öka den gemensamma utbildningen inom cybersäkerhet. EU inrättade också strax efter CCDCOE byrån EU-Lisa[19] i Tallinn, som jobbar med att samordna unionens inre säkerhet gällande it-system som hanterar känslig information.

På nationellt håll ledde attacken till att Estland inrättade ett särskilt cybersäkerhetsråd direkt under statsrådets säkerhetskommitté, med uppgiften att vara knytpunkt för samtliga myndigheter och att garantera att landets nationella cybersäkerhetsstrategi efterlevs.[20] Estland var ett av de första länderna att framarbeta en nationell cybersäkerhetsstrategi inkluderande målsättningar, hotbild och förutsättningar. De estniska cybersäkerhetsstrategierna har varit omfattande och identifierar både *priority activities* och vissa tematiska områden där cybersäkerheten kan förbättras. Estland arbetar systematiskt med att ta fram en reviderad cybersäkerhetsstrategi för fyra år åt gången. Kvantitet innebär inte alltid kvalitet, men kvantitet kan alltid vara riktgivande – Estlands senaste cybersäkerhetsstrategi utgör 72 sidor, medan Finlands senaste cybersäkerhetsstrategi från år 2019 ligger på 12 sidor.

Likt Finlands digitala kompass har Estland utarbetat sin egen digitala agenda för år 2030. Till skillnad från den digitala kompassen där cybersäkerheten är med på ett hörn så utgör cybersäkerheten en av tre huvudpunkter i Estlands digitala agenda. Dokumentet innehåller också en rad konkreta förslag till målsättningar. Bland annat ska en cybersäkerhetsspecifik tankesmedja inrättas och satsningar göras för att öka och förbättra forskningen i cybersäkerhet vid landets universitet och forskningsinstitutioner. Det utlovas också en nationell plan

19 Formellt Europeiska byrån för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa.

20 Republic of Estonia Ministry of Economic Affairs and Communications, ”Cybersecurity Strategy 2019–2022”.

för att samordna all nationell forskning och utveckling som specifikt relaterar till cybersäkerhet.[21]

En viktig del i Estlands strategi har varit att öka förståelsen för cybersäkerheten i samhället generellt. Detta har bidragit till att Estland i dag besitter en bred talangpool med förståelse både för digitalisering och cybersäkerhet. Estland står värd för flera olika konferenser, som de årliga *Digital Summit* och *Nordic-Baltic Security Summit*. Unga personer har tillgång till såväl utbildningsmöjligheter som olika evenemang inom cybersäkerhet. Från offentligt håll erbjuder TalTechs Centre for Digital Forensics and Cyber Security utbildningar och exkursioner till klasser och ungdomar. Enligt deras estimat har över 150 000 elever och studenter från 7 år och uppåt, samt över 5 000 skollärare, deltagit i deras olika program och evenemang mellan år 2017 och år 2021. För dem med ett särskilt intresse går det att avlägga både en kandidat- och en magisterexamen i cybersäkerhet vid Tallinns tekniska universitet och universitetet i Tartu. Från privat håll har företaget CTF Tech sedan flera år tillbaka stått värd för *Cyber Battle*, riktat åt personer i åldrarna 18 till 24 år. I Cyber Battle tävlar lag om att lösa olika scenarier av cyberangrepp och poängsätts utifrån sina prestationer. För årgången 2023 hölls även en regionalturnering med de andra baltiska och nordiska länderna. CTF Tech håller också olika kurser och utvecklar för tillfället en *e-learning* plattform riktad till såväl lärare som studenter.

21 Republic of Estonia Ministry of Economic Affairs and Communications, ”Estonia’s Digital Agenda 2030”, 2023.

5. Vägen framåt

Arbetet med att revidera den pågående cybersäkerhetsstrategin kommer att vara viktigt för att fastslå hur vi i Finland kan stärka vår cybersäkerhet i dag och på sikt. Nedan följer två huvudförslag med inspiration från Estland som vi gärna ser att våra beslutsfattare skulle prioritera.

Gör som Estland och investera i digitalisering och cybersäkerhet.

- **Öronmärk en större del av bnp för it- och cybersäkerhetsinvesteringar.** Likt Estlands tidiga satsningar bör Finland öka investeringarna i cybersäkerhet. Det hjälper också att stävja de skenande kostnaderna av cyberbrottslighet och att förbereda landet för kommande angrepp. Regeringen bör minimera skadekostnaderna till följd av cyberangrepp och sätta upp en gräns för Finland över vilken skadekostnaderna inte får stiga.
- **Kartlägg de faktiska skadekostnaderna till följd av cyberangrepp.** I denna rapport estimerade vi skadekostnaderna för cyberangrepp i Finland till nästan 290 miljoner euro, vilket antagligen är i underkant på grund av ett större mörkertal. Regeringen bör tillsätta en utredning för att ta reda på hur mycket cyberangreppen kostar Finland – från privat till offentlig sektor.
- **Dataambassader och säker datalagring.** Undersök möjligheten att skapa en dataambassad likt Estland, där kritiska data kan lagras utomlands med hög säkerhet. Detta skulle skydda viktiga statliga data i händelse av cyberattacker eller andra hot.
- **Tydligare ansvarsfördelning.** Involverade parter måste veta till vilken myndighet eller aktör de kan vända sig och hur man ska agera när man blir utsatt för cyberangrepp. Se över hur vi i Finland kan ta efter Estlands struktur, som ter sig mer transparent och lättförståelig.

Gör som Estland och fokusera på utbildning och forskning

- **Ge utbildningsmöjligheter i ett tidigt skede.** Konkretisera hur utbildningsväsendet kan involveras i arbetet med att öka kunskapen och kompetensen inom cyber- och datasäkerhet. Det ska vara coolt att syssla med cybersäkerhet och ett bra sätt att lyckas med det är att redan tidigt erbjuda möjligheter till utbildning.
- **Satsa på forskning och utveckling.** Undervisnings- och kulturministeriet anslår 255 miljoner euro i tilläggsfinansiering till universiteten för ett pilotprogram som antar cirka 1 000 nya doktorander mellan år 2024 och år 2027. I pilotprogrammet finns inget renodlat fokus på cybersäkerhet, trots att andra digitaliseringsfrågor ges statusen ”flaggskeppsområden”. Regeringens målsättning om att fyra procent av bnp ska läggas på forskning och innovation tyder på att pilotprogrammen har stor möjlighet att bli en del av den högre utbildningen framöver. Cybersäkerhet bör göras till ett flaggskeppsområde och delar av finansieringen bör riktas åt doktorandprogram inom cybersäkerhet.

Kommentar

Utvecklande av cybersäkerhet för företag och medborgare

Vi lever den tredje revolutionen, där digitaliseringen förändrar själva strukturen i samhällen och företag – allt som har med pengar, data och funktionalitet att göra, digitaliseras. Samtidigt förändras det sätt på vilket alla tillgångar, data och funktioner skyddas – och det är här cybersäkerheten kommer med i bilden. När allt inte kan skyddas måste statsförvaltningen prioritera hur man fördelar resurserna mest effektivt för att skydda samhällets viktigaste funktioner, till gagn för oss alla. Hur har Finland lyckats och hur kommer vi att lyckas med cybersäkerhet i framtiden?

Digitaliseringen påverkar alla i vårt samhälle, oavsett om det handlar om hälsoinformationssystem inom hälsovården och styrning av utrustning inom äldreomsorgen, företagens och medborgarnas användning av tillgångar inom bankväsendet, betalningstransaktioner för anskaffning och försäljning inom industrin, produktionsstyrning i fabrikerna eller till och med den tid som människor tillbringar i vardagen med tv-program och onlinespel, där aktuella nyheter och varningar från myndigheterna förmedlas till oss via digitala nätverk och applikationer. Så digitalisering berör allt, varje företag och organisation är nu en digital organisation, oavsett är man medveten om det eller inte. Det finns ingen enskild enhet som kan avgöra och förstå vikten av alla olika affärsfunktioner och därmed besluta om det bästa skyddet för dem alla. Digitaliseringens omvandling till en del av samhällsstrukturen kräver en motsvarande grad av inkludering.

Digitaliseringen är redan överallt – det måste cybersäkerheten också vara

I och med digitaliseringen måste skyddet av den, cybersäkerheten, finnas på allas agenda och ansvar, i allas infrastruktur. Å andra sidan är det motiverat att koncentrera tekniska förmågor för statligt skydd så, att alla har lika tillgång till tekniskt stöd. Här är Transport- och kommunikationsverkets cybersä-

kerhetscenter den digitala världens brandkår, och en anmälan dit ger första hjälpen. Precis som vid vanliga brott är polisen den aktör som utreder händelseförloppet i en brottsutredning. Centralkriminalpolisens cybercenter är specialiserad på detta vid allvarligare cyberbrott. Försvarsmaktens roll sträcker sig till krigssituationer. På många håll är gränserna mellan dessa något suddiga, och där spelar samarbetet mellan aktörerna en nyckelroll – alla behövs för ett starkt skydd.

Statlig cyberkompetens ger gemensamt skydd för medborgarnas viktiga verksamheter

Statlig cyberkompetens för att förebygga och skydda mot cyberattacker blir särskilt relevant i en situation där företaget blir samhällets försvarare. När en statlig aktör eller en kriminell organisation försöker undergräva medborgarnas kristålighet genom att försämra tillförlitligheten i kritiska tjänster eller pressa dem på pengar genom att lamslå dem, är statens förmåga att stödja företag för att skydda viktiga funktioner för medborgarna, avgörande. Eller när statlig verksamhet störs eller till och med attackeras fysiskt, med hjälp av offentliga aktörers data som finns tillgänglig online eller kritiska företags centrala kritiska flaskhalsar. Här ligger det i allas intresse att samhället har ett ansvar för att sammanföra de centrala aktörerna, säkerställa en smidig informationsgång, samt skydda verksamheten och säkerställa en smidig vardag för medborgarna.

Sektormyndigheterna har en förståelse för de kritiska tjänster som bör skyddas

När det gäller cybersäkerhet i medborgarnas vardag, delas ansvaret mellan användaren och tjänsteleverantören. En användare kan använda tjänsten digitalt eller så kan det finnas underliggande system som påverkar tjänsteproduktionen. En medborgare kan inte nämnvärt påverka driften och säkerheten av dem. I samband med konventionella tjänster är riskbedömning normal affärsverksamhet, hur mycket ett företag investerar i funktionaliteten av digitala enheter eller cyberhot. När tjänsten är samhällskritisk och kunden inte kan påverka om hen använder tjänsten eller inte, och tjänsten är en grundförutsättning för en normal vardag, har samhället ett ansvar att övervaka och främja tjänstens säkerhet vid sidan om företagets egna lösningar.

Den cybersäkerhet som samhället kräver kan genomföras med lagstadgade minimikrav eller tjänster som samhället erbjuder, och som gör det möjligt för ett företag att upprätthålla tjänstens cybersäkerhet på en god nivå. Här är sektormyndigheterna och försörjningsberedskapscentralen, med sina nätverk, bäst lämpade att identifiera de viktigaste tjänsterna som ska säkras och flaskhalsarna i dessa tjänster. Sektormyndigheter är till exempel Valvira inom hälsosektorn och Energimyndigheten inom energisektorn. Cybersäkerhetscentret kan å andra sidan tillhandahålla tjänster för lägesbild och observationstjänster, för att stödja tekniskt skydd inom alla sektorer, till exempel för att hålla allvarlig skadlig programvara under kontroll. Försörjningsberedskapscentralen finansierar utvecklingen av dessa samhällstjänster till nytta för företagen och i slutändan till nytta för medborgarnas trygghet. På så sätt kedjas den bästa kompetensen, kunskapen och färdigheterna hos alla parter samman för att skydda samhället.

Cybersäkerhet är dagens medborgerliga kamp

Medborgarna, servicekunderna och användarna har eget ansvar för att använda digitala tjänster i enlighet med principerna för informationssäkerhet. Det ligger även i tjänsteleverantörens intresse, att kunderna inte blir lurade och förlorar pengar eller data, vilket inte är bra för någons affärsverksamhet. Därför är målet att göra tjänsterna också så säkra som möjligt och att minska risken för att användaren av misstag utgör en datasäkerhetsrisk för sig själv eller tjänsteleverantören, och därmed förlorar pengar eller data för båda. Det kvarstår fortfarande risk att användaren inte sköter säkerheten för sin egen enhet enligt instruktionerna, uppdaterar informationssäkerhetskontrollerna enligt rekommendationer eller blir lurad.

Dessvärre försöker kriminella oftast hitta människonära sätt att lura användare att göra misstag – som den tidigare rapporten säger, är det en biljonaffär att ta del i allt genom digital brottslighet, där många små bedrägerier bildar en stor helhet. Ficktjuvarna har hittat bakfickornas, på kontanter tömda plånböcker, på nätet. Myndigheter och företag försöker snabbt blockera dessa medel, men även medborgarnas grundläggande säkerhetskunskaper i nya digitala strukturer är nödvändiga. I motsvarande avseende krävs, att alla har grundläggande kunskap om trafiksäkerhet, när de börjar utnyttja vägar som är i allmänt bruk.

Cybersäkerheten i Finland är bland de bästa i världen

Hur har man lyckats med detta i Finland? I den nyaste ITU-T cyberindex-rapporten[22] fick Finland fulla poäng tillsammans med elva andra länder. Cyber-attacker mot finländska företag och bedrägerier mot medborgare är vardag, men under de senaste åren har vi undvikit situationer med särskilt allvarliga samhällsrelaterade konsekvenser. Man kan säga att på en principiell nivå har det finska nätverksbaserade tillvägagångssättet visat sig vara progressivt och ge säkerhet – vi är ett modelland för cybersäkerhet tillsammans med Estland. Men i slutändan kommer säkerheten att avgöras i vardagen, hur vi arbetar tillsam-mans i takt med att digitaliseringen fortsätter att utvecklas. AI och kvantberäk-ning kommer att medföra nya cyberhot för att testa vårt system, för vilket vi har en stark strukturell och omfattande bas.

Att säkra ett ömsesidigt beroende samhälle är inte enkelt, eftersom bero-enden förändras och angripare, giriga på pengar eller data, försöker slå till mot de sårbarheter som lämnats utan tydligt ansvar och skydd. Ingen part kan kontrollera allt kunskapskapital, så samarbete är en nödvändig förutsättning. När det gäller säkerhet är struktur ett sätt att organisera och kan göras bra och dåligt på många sätt, men i slutändan är det inställningen som avgör om man lyckas: vill vi lyckas tillsammans? Att prestera på bästa möjliga sätt utifrån sitt eget ansvar och hjälpa sin partner att lyckas med sitt? Med rätta attityder är det mentala kapitalet starkt, och den digitala toleransen garanterad. Cybersäkerhet stöder mental kristålighet – vad som än händer, var det än händer, kommer vi att ta oss igenom det tillsammans.

Jarna Hartikainen
Enhetsdirektör
Planering för beredskap
Försörjningsberedskapscentralen

22 https://www.itu.int/dms_pub/itu-d/opb/hdb/d-hdb-gci.01-2024-pdf-e.pdf

Källförteckning

Allianz, ”Risk Barometer – Identifying the major business risks for 2023”, 2022.

Andrew Kramer/The New York Times, ”Hackers Bring Down Government Sites in Ukraine”, 2022.

Dann Pettersson/Hufvudstadsbladet, ”Finnair pausar flyg efter gps-störningar”, 2024.

ESET Research, ”IsaacWiper and HermeticWizard: New wiper and worm targeting Ukraine”, We Live Security, 2022.

Finanssiala Ry, ”Varo, varmista ja varoita: Nettihuijaukset ja tietojenkalastelu muuttavat muotoaan, mutta niiltä on mahdollista suojautua”, 2022.

Mai Periman, ”How to prevent the bank robbery no one can see”, Cisco, 2017.

Markku Korhonen/Cryptonews, ”Valtavaa kasvua: Digihuijaukset Suomessa lisääntyivät”, 2024.

Niklas Fagerström, ”Finländare har lurats på rekordmycket pengar på nätet – det handlar om tiotals miljoner euro på ett halvår”, Yle, 2023.

Republic of Estonia Ministry of Economic Affairs and Communications, ”Estonia’s Digital Agenda 2030”, 2023.

Republic of Estonia Ministry of Economic Affairs and Communications, ”Cybersecurity Strategy 2019–2022”.

Statistikcentralen, ”Befolkningens användning av informations- och kommunikationsteknik”.

Statsrådet, ”Utredning: Finlands cybersäkerhet bör utvecklas målmedvetet och myndigheternas samarbete och processer förbättras ytterligare”, 2023.

Steve Morgan/Cybercrime Magazine, ”Cybercrime to cost the world $10.5 trillion annually by 2025”, 2020.

Stockholms Handelskammare, ”Cyberbrott mot svenska företag – hur bygger vi en säkrare framtid?”, 2022.

Säkerhetskommittén, ”Strategi för cybersäkerheten i Finland 2019”, 2019.

Säkerhetskommittén, ”Strategi för cybersäkerheten i Finland”, 2013.

Traficom Cybersäkerhetscentret, ”Nationella samordningscentrumets uppgifter”, 2023.

40 miljoner euro. Uppskattningsvis så mycket pengar blev vi lurade på över nätet ifjol. Sedan 2019 har antalet fall där finländare råkat ut för nätbedrägerier ökat explosionsartat: år 2023 gjordes över 7000 anmälningar till polisen.

På nätet är det inte bara kriminella individer och ligor som åsamkar medborgarna huvudbry. I allt större utsträckning står även enskilda stater bakom cyberbrottsligheten. Och där det inga gränser finns, kan vem som helst råka illa ut.

Nationalekonomen **Theo Herold** (Svenska Handelshögskolan) ger en inblick i vad cyberbrottslighet är och hur mycket det kostar Finland, vad som görs för att förbättra cybersäkerheten samt vad vi kunde lära oss av Estland, som ligger steget före i mångt och mycket som gäller den digitala sfären.

Rapporten presenterar även konkreta åtgärder för förbättrad cybersäkerhet samt en kommentar av Försörjningsberedskapscentralen om hur individen och staten kan stärka cybersäkerheten.

AGENDA
TANKESMEDJAN • AJATUSHAUTOMO