Transport- och kommunikationsverket
Cybersäkerhetscentret

INFORMATIONSSÄKERHET 2019

Cybersäkerhetscentrets årsrapport

Traficoms publikationer

5/2020

INNEHÅLL

Samhället behöver datasäkra vardagliga handlingar - tillsammans är vi den starkaste länken

År 2019 fördes den mest omfattande samhällsdebatten om 5G-teknologins cybersäkerhet. Vi var beredda på det eftersom våra experter har bedömt att den nya teknologin och standarden medför tekniska utmaningar och möjligheter redan från och med 2017. Vår förmåga att producera teknisk information för den nationella riskbedömningen var också värdefull internationellt.

Till våra höjdpunkter hörde också våra internationella evenemang: världens första 5G Hackathon och Galileo Innovation Challenge. Händelserna visade att samarbetet mellan teleoperatörer, tillverkare och myndigheter har varit smidigt. Samarbete är en styrka som vi måste hålla fast vid.

Det gångna året kommer också att ihågkommas för det snabba utnyttjandet av nya sårbarheter, omfattande utpressningsprogram och vändningen då bedrägerier och informationsfiske blev vardag – det nya normala. Bakom detta ligger också ett superår när det kommer till regleringen av cybersäkerheten, då flera lagar om informationssäkerhet trädde i kraft. Bland annat blev TUPAS föråldrat och ändringarna i identifierings- och betrodda tjänster gav konkurrens till identifieringstjänsterna.

Årets mest synliga cyberväckare var cyberattackerna mot kommunsektorn. De visade att vårt samhälle är sårbart och störde bland annat medborgarnas basservice och vardag. Fallen och de utredningar som gjorts utifrån dem har väckt diskussion inom statsförvaltningen, kommunerna och företagsvärldens högsta ledning. Det är ytterst viktigt att frågan inte bara diskuteras, utan att man för att förbättra situationen vidtar nödvändiga och konkreta åtgärder och fattar beslut.

År 2019 lanserades ett nytt betydande fenomen i Finland, "big game hunting", där brottslingar är ute efter stora lösensummor genom attacker med utpressningsprogram som riktas till stora företag. Attackerna har medfört allvarliga störningar i verksamheten och till och med avbrott samt omfattande ekonomiska förluster för företagen. Fenomenet har lyft upp en övergripande hantering av cyberriskerna, som även beaktar leveranskedjorna och samarbetspartnerna.

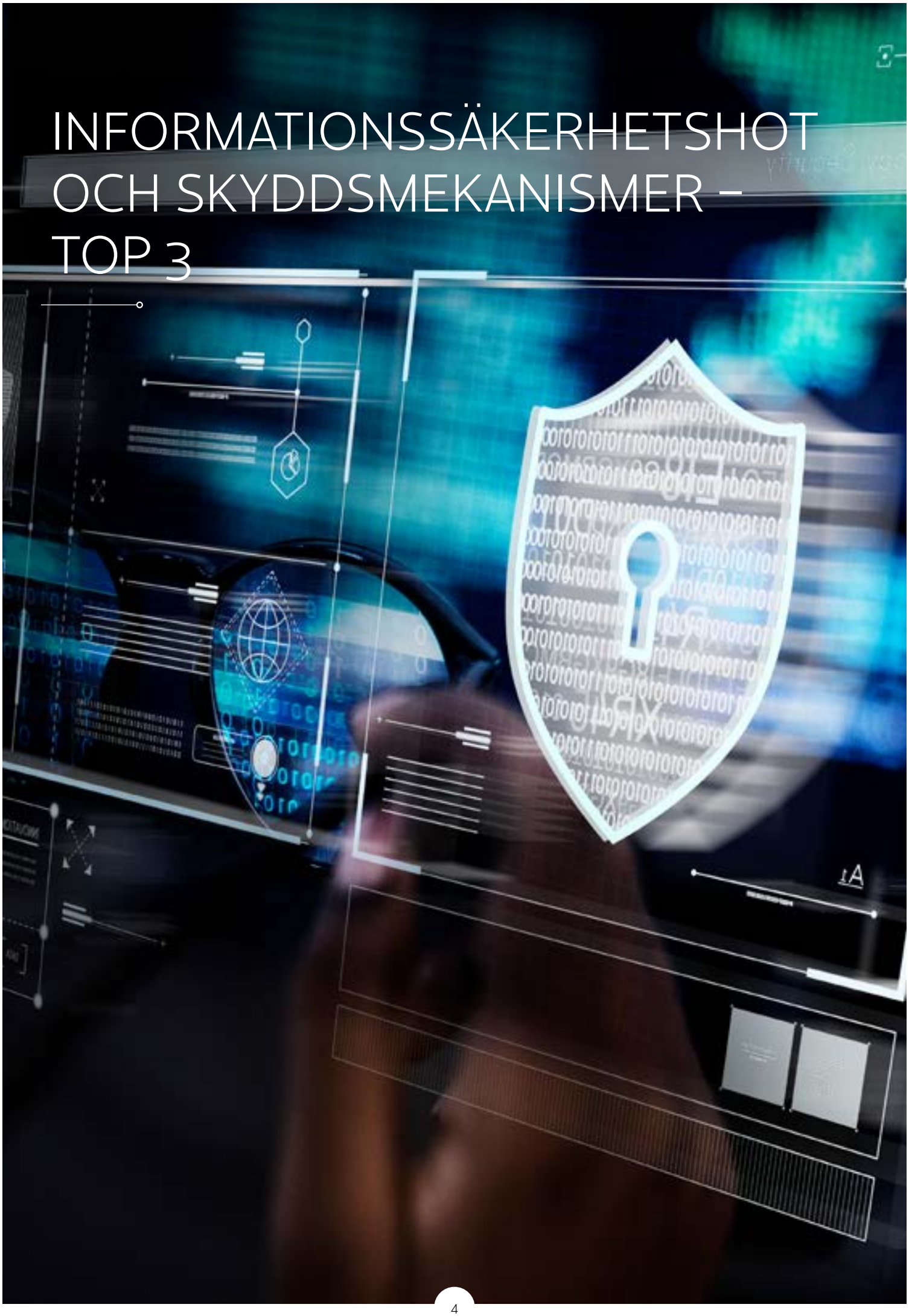
Cybersäkerhetsmärket, som vi utvecklade för att trygga konsumentutrustningen i fjol, fick glädjande stor publicitet. Märket erbjuder människor ett enkelt sätt att förbättra sin personliga cybersäkerhet. Vi höll kampanjer i sociala medier, TV och radio och nådde över 2,4 miljoner medborgare. En aktiv medborgarkampanj fick människor att intressera sig för informationssäkerhet!

Det kommande året medför både nya utmaningar och positiv utveckling. Intresset för den cybersäkerhetguide för företagsstyrelser som publicerades i början av året är ett gott tecken på viljan att vidta åtgärder.

Jag har haft nöjet att börja som direktör för Cybersäkerhetscentret i början av 2020. Aktiv verksamhet med våra intressentgrupper erbjuder en utmärkt grund för utvecklingen av cybersäkerheten i samhället även 2020.

Helsingfors 19.2.2020,
Kalle Luukkainen
Överdirektör
Cybersäkerhetscentret
Transport- och kommunikationsverket Traficom

INFORMATIONSSÄKERHETSHOT OCH SKYDDSMEKANISMER – TOP 3



Hot och lösningar för privatpersoner

Bra lösenord, regelbundna uppdateringar av informationssäkerheten och genomtänkt beteende på internet. Under de närmaste åren förändras datasäkerhetshoten mot privatpersoner och lösningarna mot dem knappt. Med samma principer skyddar du dig själv och dina viktigaste uppgifter nu och under de kommande åren.

HOT

Bluffmeddelanden tar dina uppgifter och pengar

Alla blir föremål för bedrägerier och nätfiske. Bedrägerier drabbar dagligen såväl företag, den offentliga förvaltningen, föreningar, fonder, stiftelser som läroanstalter. Bedrägerierna kan vara uppenbara eller helt trovärdiga, skickligt gjorda och riktade. Med hjälp av bedrägerier försöker brottslingar få tillgång till organisationers datasystem med målet att till exempel skicka falska fakturor eller utreda affärshemligheter.

Dåliga lösenord och lätt åtkomst till elektroniska tjänster

Vi kan ha hundratals webbtjänster till vårt förfogande. Eftersom många unika lösenord inte går att komma ihåg, blir det lätt att man använder samma enkla lösenord i flera tjänster. Detta ökar riskerna när alla konton som skyddas med samma lösenord vid dataintrång eller dataläckage är i fara.

Oskyddade smarta enheter

Din mobil, smart-tv och dator innehåller säkert värdefull information om dig. Kan du sköta deras säkerhet och uppdateringar? En stor del av uppdateringarna av informationssäkerheten innehåller korrigeringar för att åtgärda säkerhetsbrister i enheten eller programvaran. Det är alltid riskfyllt att använda en ouppdaterad enhet. Samtidigt bjuder du in till dataintrång.

LÖSNINGAR

Alla uppgifter behöver inte anges

En myndighet eller tjänsteleverantör ber inte om dina användarnamn eller bankkoder på nätet. Om någon plötsligt frågar efter dina uppgifter kan du fråga varför och fundera på om meddelandet är äkta. Använd inte länken du fått, utan logga in i tjänsten via tjänsteleverantörens sidor. På så sätt kan du tryggt kontrollera om dina uppgifter verkligen behövs och om du behöver göra någonting.

Skydda dina uppgifter med bra lösenord och stark autentisering

Ett bra lösenord är åtminstone långt. Använd aldrig samma lösenord i flera tjänster. Ta i bruk en lösenordshanterare. Det kommer ihåg lösenorden åt dig. Börja också använda 2-stegsidentifiering och stark autentisering alltid när det är möjligt. På så sätt tryggar du till exempel ditt bankkonto och dina konton på sociala medier bättre.

Sköt om uppdateringar och produktsäkerhet

Genom att uppdatera din utrustning och hålla den uppdaterad skyddar du den också mot hot mot informationssäkerheten. När du tar i bruk automatiska uppdateringar behöver du inte komma ihåg dem själv.

Ska du skaffa en ny smart enhet?
Cybersäkerhetsmärket vittnar om anordningens säkerhet.

Hot och lösningar för organisationer

Cybersäkerheten inom organisationen syns i riskhanteringen, beredskapen och personalutbildningen. Helheten består av att behärska många olika delområden och därför borde cybersäkerheten vara hela arbetsgemenskapens verksamhetssätt.

HOT

Dagligt nätfiske och bedrägerier

Bedrägerier och nätfiske riktas dagligen till företag, offentlig förvaltning, föreningar, fonder, stiftelser och läroanstalter. De kan vara uppenbara eller helt trovärdiga, skickligt gjorda och riktade. Med hjälp av bedrägerier försöker brottslingarna få tillgång till organisationens datasystem med målet att till exempel skicka falska fakturor eller utreda affärshemligheter.

Snabb användning av nya sårbarheter - traditionella bekämpningsmetoder räcker inte längre

Brottslingar utnyttjar nästan omedelbart sårbarheter som avslöjats i deras attacker. Organisationer måste vara beredda på att uppdatera sina datasystem och applikationer allt snabbare. Detta gäller i synnerhet organisationer som arbetar med högteknologi och innovationer och som är särskilt bevakade av både brottslingar och industrispioner. Känner ni till er informationsmiljö och de tillämpningar och system ni använder? Utan denna information kan attacker mot er informationsmiljö inte bekämpas till exempel genom att uppdatera informationssäkerheten.

Tjänster centraliseras och läggs ut på entreprenad utan planering och ansvarsfördelning

Utläggning av centrala tjänster eller tillhandahållande av tjänster till samarbetspartner ökar risken för en cyberattack. Brottslingar utnyttjar partner eller underleverantörer när de försöker komma in i informationssystemen för sitt egentliga mål, bland annat genom att stjäla användarrättigheter som överlåtits till en partner. Olika störningssituationer kan sprida sig på ett omfattande och överraskande sätt till platser där centraliseringen eller utkontrakteringen av de egna tjänsterna inte har planerats ordentligt.

LÖSNINGAR

Förankra cybersäkerheten i er riskhantering

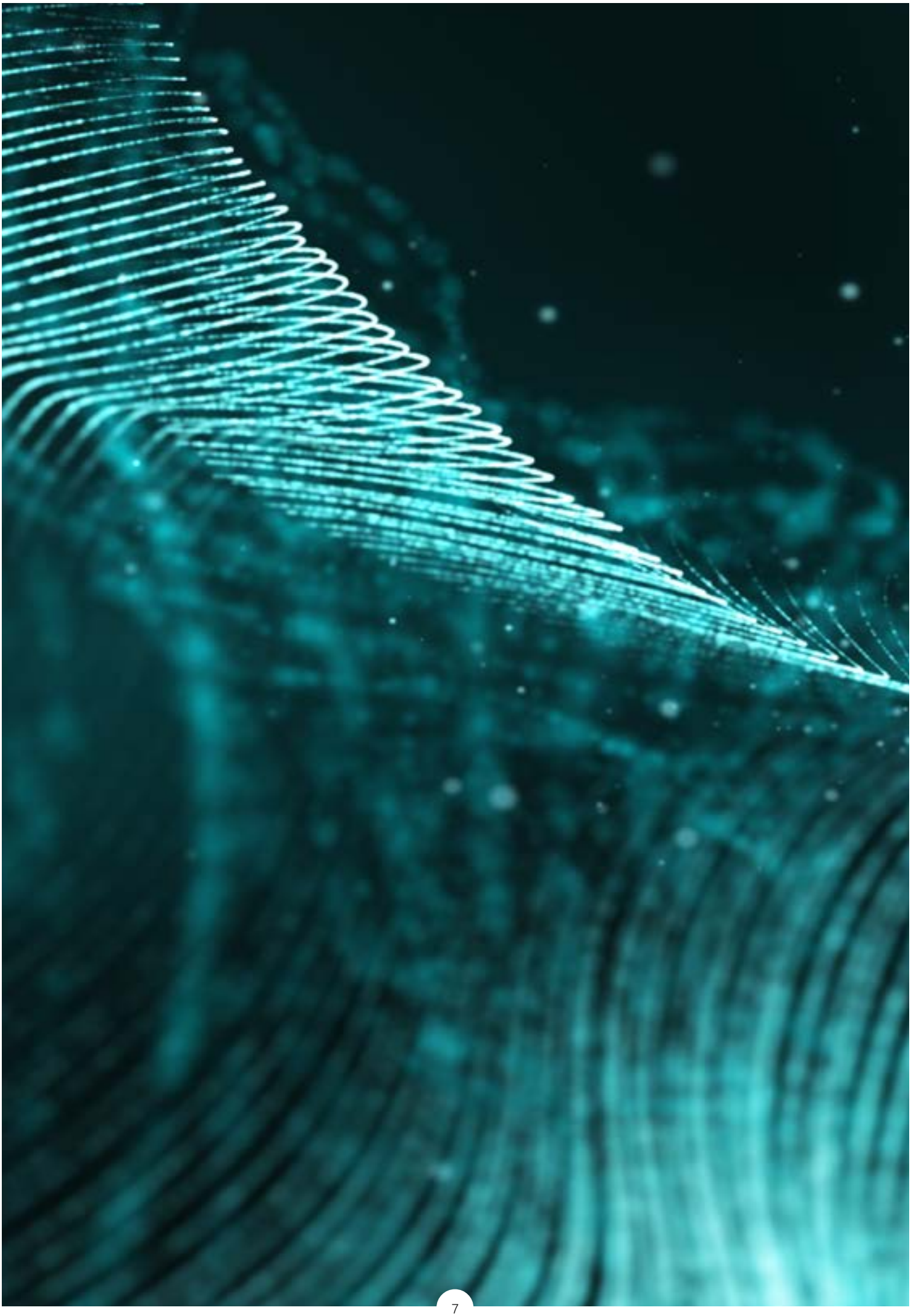
Cybersäkerhetsriskerna måste beaktas. För riskerna gäller samma mekanismer som för mer traditionella risker: risken kan elimineras till exempel genom att ta tjänsten ur bruk eller minska sannolikheten genom att använda stark autentisering. Den återstående risken är acceptabel när den ligger på en nivå som organisationens ledning kan godkänna.

Öva på att agera vid störningar och avvikelser

Vad gör ni om en nätbrottsling har lyckats hacka er e-post och skicka bluffakturor i ert namn? Genom att utbilda er och öva på olika cyberstörningar utreder ni bästa praxis. Ofta är detta också det billigaste sättet att upptäcka brister. Om ni känner till er egen informationsmiljö och har övat till exempel på rutinerna för uppdatering och säkerhetskopiering av systemen, kommer ni att klara er bättre både under övningarna och i verkliga kriser.

Ge leverantörerna ansvar och ta reda på vilka kopplingar era tjänster har

Leverantörernas ansvar, åtgärder vid avvikelser och kopplingar i anslutning till era tjänster måste ni känna till innan de läggs ut på entreprenad. Kom överens om verksamhetsmodeller och ansvar med era partner och tredje part redan i avtalsförhandlingarna. På så sätt känner ni till er roll, ert ansvar och varandras handlingssätt om till exempel en störningssituation inträffar.



Betydande cyberhändelser 2019

POSITIVA RESULTAT

- **Säkerheten hos nya teknologier byggs upp:**
  - 5G Hackathon
  - Galileo Innovation Challenge
- **Effekter av projektet KYBER 2020:**
  - Träningen i cybersäkerhet har ökat i organisationerna - Från vår övningsanvisning tar man grunderna för träningen i besittning.
- **Medborgarnas informationssäkerhetsmedvetenhet och -färdigheter i bättre skick:**
  - Cybersäkerhetsmärket
  - Säkerhetsisterna
  - Guiderna Tryggt på webben för barn och föräldrar (på finska)
  - Spoofy - barnens eget informationssäkerhetsspel
- **Cybersäkerheten inom den kritiska infrastrukturen utvecklas:**
  - Mätaren Kybermittari för bedömning av cybersäkerhetsnivån
  - HAVARO-tjänsten
  - DNSSEC

INTRESSANTA FENOMEN

- **Skadeprogrammet QSnatch**
- **Speglande överbelastningsangrepp**
- **Lyckat val och EU-ordförandeskapsperioden**

OROVÄCKANDE

- **Nya normala: Dataintrång och nätfiske via Office 365**
- **Big game hunting - nätbrottslingar som jagar stora byten**
- **Kommunernas cybersäkerhet**

ÄNDRINGAR I INFORMATIONSSÄKERHETSKRAVEN

- **TUPAS är historia**
- **Konkurrens på marknaden för identifieringstjänster**
- **Stöd för upphandling av molntjänster enligt våra kriterier**

CYBERVÄDERFENOMEN

Nätverkens funktion

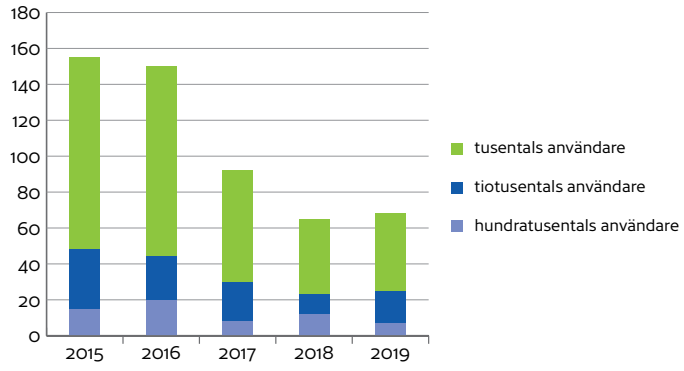
Stormvindar och blixtar avbröt samtal och internet-anslutningar

De långvarigaste störningarna 2019 började med väderförhållandena. I januari bröt stormen Aapeli elektriciteten och orsakade flera långvariga funktionsstörningar. I juni förstörde strömavbrott som orsakades av blixtar flera kraftverkssystem i kommunikationsnätet och orsakade flera betydande funktionsstörningar. Fel i kraftverkssystemen som orsakas av blixten kan inte helt undvikas, men ofta förhindrar skydd mot överspänning kommunikationsnätets komponenter från att förstöras.

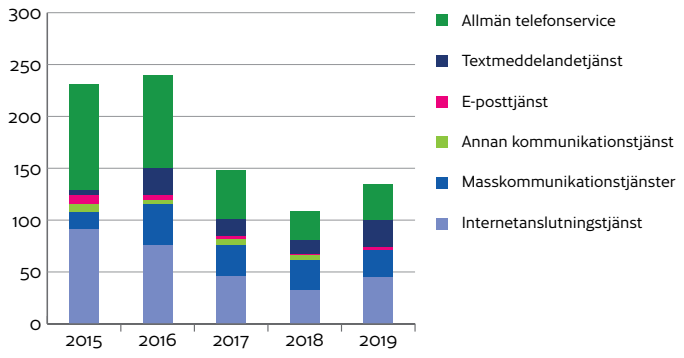
Inom de inhemska kommunikationstjänsterna har antalet allvarligaste störningar halverats sedan 2018. I synnerhet har de omfattande och allvarliga felen i antenn-TV-nätet minskat. Däremot ökade de störningar som påverkade cirka 1 000–10 000 användare av kommunikationstjänster något jämfört med 2018. De största störningarna uppstod genom olika fel i apparatur och programvara samt elavbrott. Det totala antalet betydande störningar har dock minskat tydligt från åren 2015 och 2016.

Enligt vår bedömning har det årliga antalet betydande funktionsstörningar minskat åtminstone av följande orsaker:

- de stora förändringarna i de allmänna kommunikationsnäten har minskat
- med ändringsarbeten har teleföretagen åstadkommit nätverk och tjänster som är mer hanterbara och som har högre feltolerans
- de centrala datakommunikationskablarna bryts allt mer sällan av vid grävarbeten
- samarbetet mellan teleföretag och elnätsbolag har förbättrats.



Betydande störningar enligt antalet användare av kommunikationstjänsterna åren 2015–2019.



Betydande störningar per kommunikationstjänst åren 2015–2019. En störning kan påverka flera kommunikationstjänster på en gång.

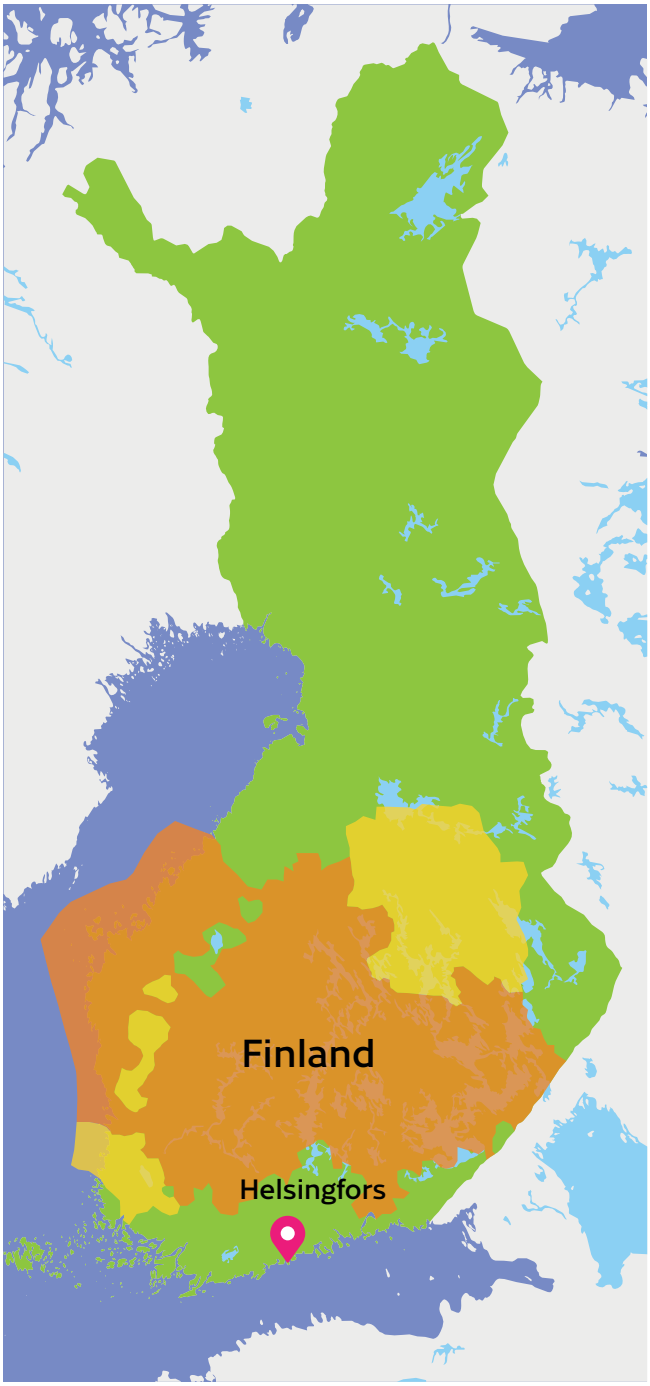
Aapelis rekordartade vindar orsakade strömavbrott hos 120 000 kunder

Stormen Aapeli påverkade landskapen Österbotten och Åland kraftigast den 1 och 2 januari 2019. Den hårda vinden fällde många träd som när de föll på elledningarna bröts elektriciteten i de apparater som höll mobilnäten i drift. I över en tredjedel av Finland förekom betydande störningar i de mobila tjänsterna. Även myndighetsradionätet VIRVE drabbades av störningar. För det fasta telefonnätet och TV orsakade stormen inga betydande störningar.

På Åland var Ålands radio utan ström i ett par timmar. Enligt nyhetsuppgifterna var även nödtrafiken bruten i nästan ett dygn. I Fastlandsfinland kunde det finnas lokala skuggor som överlappade varandra, därför var det ställvis inte möjligt att ringa nödsamtal med mobiltelefon. Enligt Nödcentralsverket var antalet inkomna nödsamtal dock förväntat stort, så de eventuella skuggområdena hade varit små.

Störningarna i mobilkommunikationstjänsterna var som störst på onsdagsmorgonen den 2 januari 2019. I Fastlandsfinland kunde betydande störningar åtgärdas senast den 3 januari. Situationen för Ålands allmänna kommunikationstjänster förblev oklar. Enligt tidningarna förekom det fortfarande betydande störningar den 4 januari.

På grund av Aapeli saknade cirka 120 000 hushåll eller kunder el. Som jämförelse orsakade stormarna Rauli (2018) och Seija (2013) strömavbrott hos cirka 200 000 kunder. Trots rekordhårda vindar fick Aapeli mindre följder än tidigare år. För utvecklingen kan vi tacka tele- och elbolagen samt myndigheterna för ett fungerande samarbete som har blivit smidigare för varje år. Man har lärt sig av stormarna och fördelarna med samarbete.



Utsikt från Traficoms offentliga MONITORI-tjänst 2.1.2019 kl. 10.31. De olika teleföretagens störningsområden är markerade med olika nyanser av gult. Två teleföretags tjänster har försvagats avsevärt.

Funktionssäkerhet för övriga ICT-tjänster

Betydande störningar i såväl den offentliga förvaltningens som företagens ICT-tjänster har färgats av att planerna inte har fungerat i praktiken trots att åtgärder som förbättrar funktionssäkerheten har planerats.

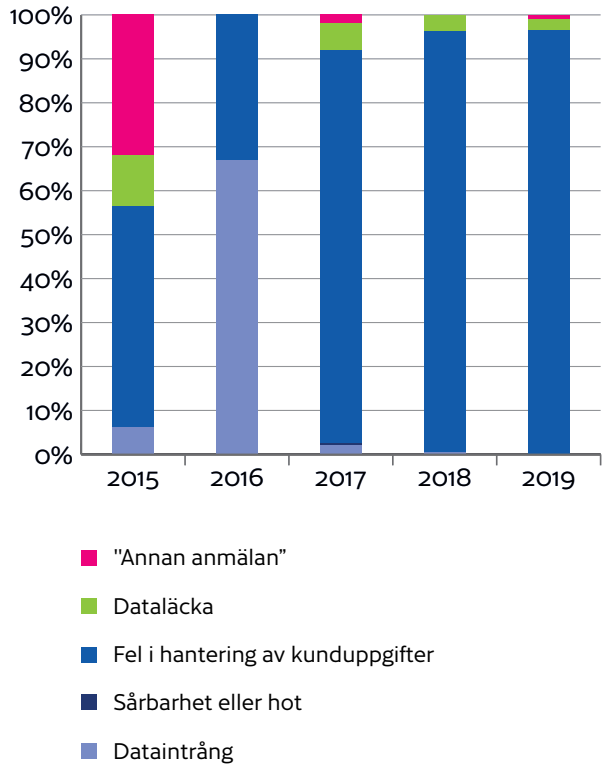
Särskilt inom hälso- och sjukvården har störningarna betydande konsekvenser, även om man har förberett sig på att vårda kunder utan datakommunikationsförbindelser. ICT-störningar fördröjer hälso- och sjukvårdens verksamhet och serviceförmåga till exempel i vårdsituationer där man inte får tillgång till patientuppgifter.

Antalet anmälningar om datasäkerhetsincidenter hos teleföretag har stabiliserats

Efter de senaste årens kraftiga ökning har antalet informationssäkerhetsincidenter som anmälts till vårt ämbetsverk stannat upp och till och med sjunkit något jämfört med nivån 2018.

Anmälningar om informationssäkerhetsincidenter gäller fall där personuppgifter förstörs, försvinner, ändras eller överlåts av misstag eller olovligt. Den vanligaste anmälan har att göra med ett fel i behandlingen av personuppgifter där en enskild kunds personuppgifter hamnar i fel persons händer eller avslöjas för fel person.

Här beskrivs teleföretagens anmälningar om kränkningar av personuppgifter och deras utveckling åren 2015–2019.



Juli 2019

10.7. Patientdatasystemet Apotti var ur bruk på grund av ett fel i nätverksväxeln i Kemi stads interna nät.

11.–18.7. Det europeiska satellitbaserade positioneringssystemet Galileo fungerade intepå en vecka. Orsaken var fel i systemets båda markstationer, vilket gjorde att satelliternas exakta position på omloppsbanorna inte kunde beräknas.

September 2019

I september återställdes det gamla nödcentralssystemet ELS i en vecka för att säkerställa Erica-systemets användbarhet. Erica har upprepade gånger lidit av störningar i statens säkerhetsnät TUVE.

27.9. Patientdatasystemet Apotti ur bruk i Vanda när datakommunikationsfibern brutits av.

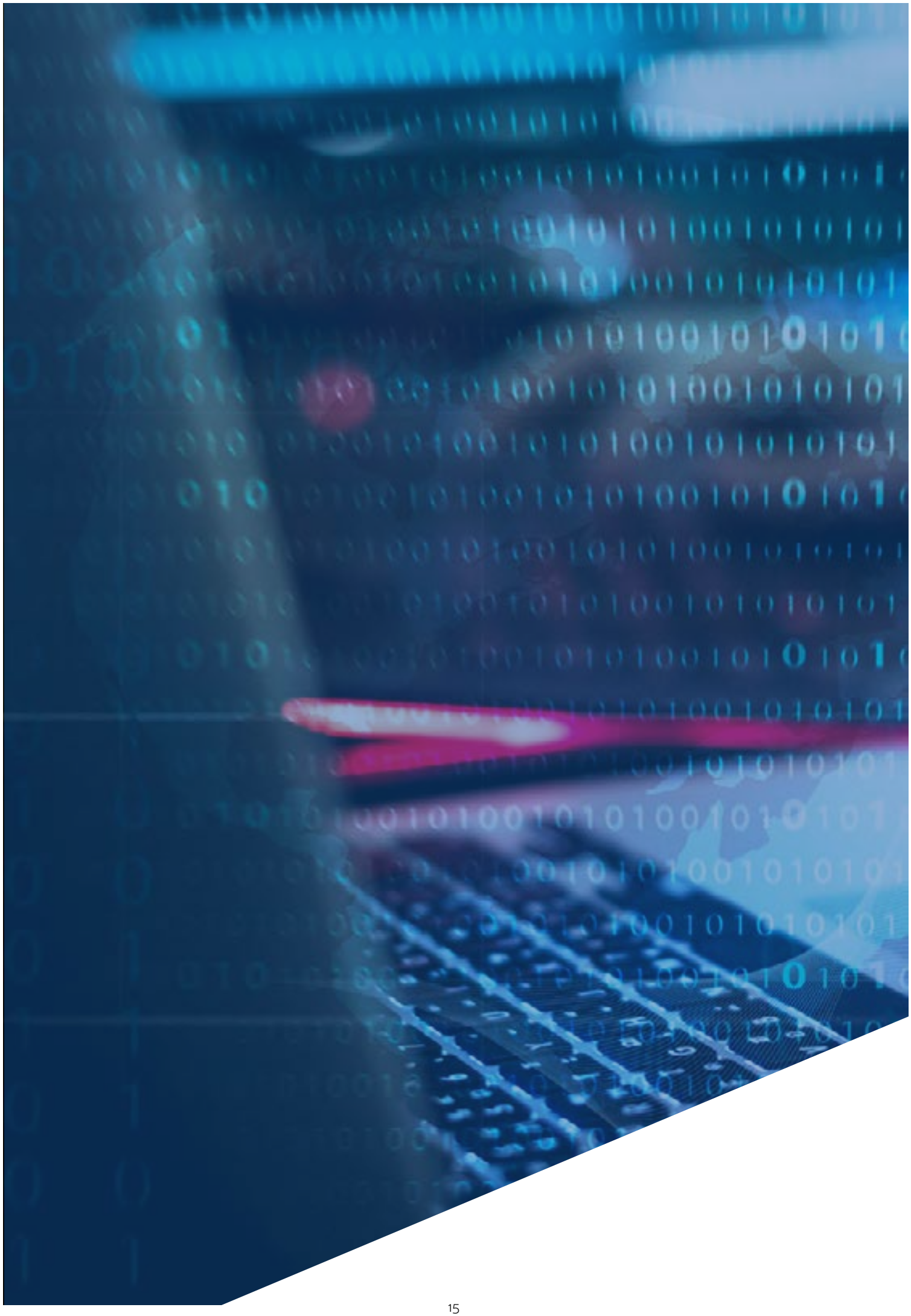
Oktober 2019

I oktober drabbades den offentliga förvaltningens ICT-tjänster av flera störningar:

10.–18.10. Störningar i Befolkningsregistercentralens BDS-gränssnitt störde flera myndigheters arbete.

13.–14.10. Störningar i stamnätet VY-verkko som upprätthålls av Valtori hindrade flera statliga myndigheters webbplatser och e-tjänster från att fungera.

14.10. En funktionsstörning i Nestes datasystem minskade tillfälligt värdet på bolagets aktier. Störningen berodde på ett fel i utrustningen i datacentralen hos den ICT-tjänsteleverantör som Neste använder.



Överbelastningsangrepp: motivet ofta trakasserier eller utpressning

I synnerhet de inhemska företagens beredskap för överbelastningsangrepp har förbättrats. Det syntes fler attacker i teleföretagens nät än året innan, men effekterna av de attacker som anmäldes till oss blev mindre.

Kvantitativt är korta attacker mycket vanliga. År 2019 varade cirka 80 procent av alla attacker i Finland i mindre än 15 minuter. Föremålen för attackerna varierar, men ett objekt som framhävs år efter år är skolornas Wilma-system. Bakom de korta attackerna kan det finnas unga som testar överbelastningsangrepp och effekterna av dem. Att göra eller försöka göra en blockeringsattack kan tolkas som ett brott som kan leda till böter för gärningsmannen eller fängelse i högst två år.

ORSAKER TILL ÖVERBELASTNINGSANGREPP

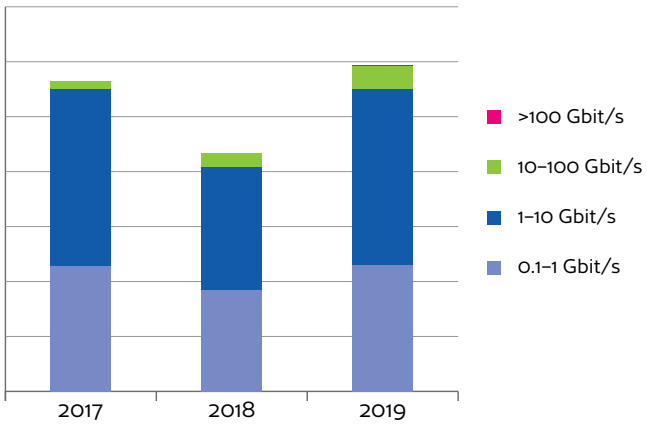
1. Störning
2. Ekonomisk vinning genom att hota med angrepp
3. Vilja och intresse att testa effekterna av en attack

Det är tekniskt sett enkelt att utföra attacker eftersom det på internet finns så kallade stresser-tjänster man kan köpa attacker från som en tjänst utan att ha egen teknisk kompetens. Flera webbplatser som säljer attacker erbjuder korta testattacker gratis.

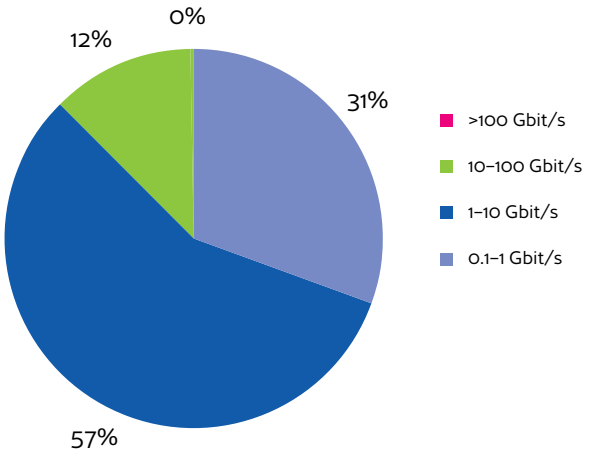
Organisationerna skyddar sig bättre än tidigare, ändå har störningar inte kunnat undvikas

I synnerhet stora finländska organisationer är bättre förberedda på överbelastningsangrepp än tidigare år. Till exempel har införandet av pakettvättjänster och molntjänster lett till att man ofta lyckas bekämpa attacker utan betydande konsekvenser för tjänsternas funktion.

Trots detta förekommer det ibland störningar i tjänsterna trots de skydd som införskaffats. I allmänhet beror störningarna på attacker som hinner slå ut tjänsterna innan bekämpningsåtgärderna aktiveras. I många fall är till exempel objektets brandvägg överbelastad och återgår inte längre automatiskt till normalläge ens efter att den egentliga anfallstrafiken inte längre når sitt mål. Det lönar sig att testa den egna organisationens förmåga att tåla attacker, så att eventuella flaskhalsar i tjänsten eller andra svaga punkter kan hittas på ett kontrollerat sätt. Ett bra exempel på detta är LokalTapiolas övning, som **Leo Niemelä** berättar om i gästpennan.



Utveckling av antalet överbelastningsangrepp i Finland.
Källa: Telia



Fördelning av antalet överbelastningsangrepp i Finland 2019.
Källa: Telia

Antalet överbelastningsangrepp har ökat jämfört med året innan. Den största ökningen har varit i attacker över 1 Gbit/s och över 10 Gbit/s.

Cirka 69 % av alla attacker är över 1 Gbit/s och 12 % över 10 Gbit/s. I Finland ser man attacker med en volym på över 10 Gbit/s och flera mindre attacker dagligen.

”DoS-övningen är ett fördärv för dem som utför överbelastnings-angrepp

På LokalTapiola har vi redan i flera år strävat efter att utveckla vår informationssäkerhet på ett fördomsfritt sätt. Bland våra verksamhetssätt har bland annat samarbetet med white hat hackers, belöningsprogrammet bug bounty och öppen kommunikation om datasäkerhet etablerat sig. I år kunde vi genomföra en överbelastningsangrepp på våra egna webbtjänster.

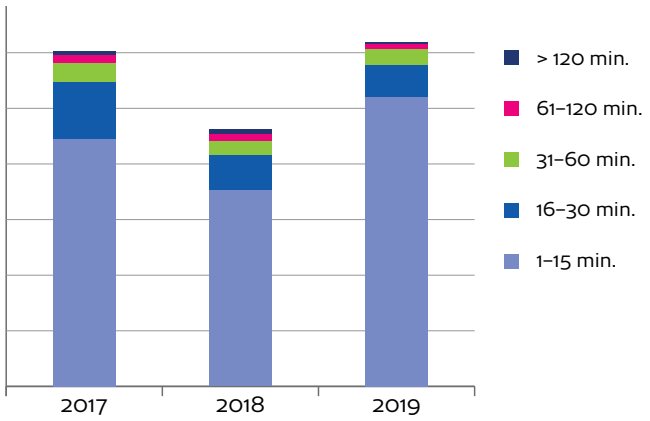
Vi attackerade våra egna webbtjänster i januari 2019 med samma verktyg som nätbrottslingar. Vi belastade våra webbtjänster allt vad vi kunde: hundratals attackdatorer hade ställts in globalt i syfte att slå ut LokalTapiolas e-tjänster. Vår avsikt var att få förmågan att bekämpa överbelastningsangrepp samt att lära oss hur LokalTapiolas infrastruktur klarar belastning som avviker från det normala nätbeteendet.

Övningen krävde mycket förhandsplanering för datakommunikationen, infrastrukturen, servrarna, applikationerna och databaserna. Vi var tvungna att uppskatta största delen av riskerna och acceptera att alla risker som övningen orsakade inte kan förutses. Beredningen, planeringen, informationen och själva genomförandet av övningen kräver planering i månader, mod från ledningen och – viktigast av allt – att övningen ses som en investering för framtiden.

Tjänster för att bekämpa överbelastningsangrepp r är ett fördärv för angripare. Bekämpningstjänster kräver dock mycket noggrann optimering och konfigurering för att fungera, så att även små attacker som bromsar upp tjänsterna kan upptäcks och förhindras från i den normala datakommunikationen. Vi lär oss att många tjänster slås ut av överraskande små trafikmängder.

Jag uppmuntrar företag att genomföra praktiska övningar eftersom de hjälper till att dimensionera försvarsåtgärderna på rätt nivå och förstå konkret vilka riskområden som organisationen bör fästa särskild uppmärksamhet vid.

Leo Niemelä
LokalTapiola



Utveckling av överbelastningsangreppens varaktighet i Finland.
Källa: Telia

Antalet attacker som varar i mindre än 15 minuter har ökat jämfört med året innan. Korta attacker under 15 minuter är sannolikt gratis testattacker som erbjuds av stresser-tjänster.

Angreppens varaktighet påverkas mest av de bekämpningsåtgärder som vidtagits, eftersom brottslingarna i allmänhet fortsätter sin attack tills den har synliga konsekvenser för målets verksamhet.

ÖVERBELASTNINGSANGREPPENS TEKNIK 2019

Liksom tidigare år bestod största delen av överbelastningsangreppen av så kallade UDP (User Datagram Protocol) -amplifikationsattacker, som till exempel utnyttjade tids- eller namntjänster. I amplifikationen används öppna servrar runt om i världen, varifrån trafiken speglas förstärkt mot målet för attacken. Attacker på applikationsnivå förekom också regelbundet.

Som en växande trend, särskilt i slutet av året, observerade vi från spegling av handskakningstrafiken TCP (Transmission Control Protocol) mot den organisation som var mål för attacken. Antalet paket var så stort att de orsakade störningar även på finländska servrar som användes vid speglingen, även om de inte var mål för attacken. Det har också varit en utmaning att bekämpa dessa attacker, eftersom de som utförde attackerna bombarderade flera av målets webbadresser samtidigt.

Spionage och påverkan

Under 2019 var utvecklingen av statligt cyberspionage i huvudsak densamma som under tidigare år. Även finländska företag och organisationer inom den offentliga förvaltningen är fortfarande föremål för cyberspionage av både politiska och ekonomiska skäl.

Världen har redan tidigare sett hur riktade cyberoperationer i värsta fall har orsakat betydande konsekvenser. Man har också sett tecken på intresse för Finlands kritiska infrastruktur. I organisationernas system söker man svaga punkter och samtidigt fotfäste i dem. Man kan också sträva efter att få tillgång till systemen genom riktat fiske efter användarnamn.

Cyberspionage hjälper till att förbättra den ekonomiska ställningen

Under året var det igen aktuellt med industrispionage i syfte att stjäla företagens kunskapskapital. Genom att stjäla information som är betydelsefull för affärsverksamheten strävar man efter ett ekonomiskt försprång till exempel genom att dra nytta av andras utvecklings- och forskningsarbete. För den som är föremål för spionage kan det till exempel innebära försämrad försäljning eller marknadsställning, när konkurrerande produkter eller tjänster som produceras billigare till följd av spionage tar över marknaden.

Stater kan försöka förbättra sin ekonomiska ställning eller uppnå andra nationella mål samtidigt med hjälp av cyberspionage och investeringar eller annat ekonomiskt inflytande. Till exempel riktades 2019 flera anklagelser mot Kina om spionage inom luftfartsindustrin och kopiering av teknologi för att starta egen flygplansproduktion i landet.

Metoderna utvecklas så att de är svåra att upptäcka

Utnyttjandet av olika offentliga tjänster inom cyberspionage blev klart vanligare. Om angriparen lägger till sitt eget innehåll, bland annat dolda instruktioner, till exempel i bild-, video- eller molntjänster, är det svårt att upptäcka det med de sedvanliga metoder som används för att observera webbtrafiken.

Bland annat när dessa metoder blir vanligare framhävs betydelsen av observation på huvudenheterna. Ibruktagandet av lösningarna har dock varit långsam, även om det finns tillgång till både kommersiella och avgiftsfria lösningar.

En leveranskedjeattack kan vara omärkbar

Att nå det egentliga målet genom att utnyttja leveranskedjor är fortfarande ett aktuellt hot. Man kan göra intrång eller komma åt uppgifter till exempel genom att göra intrång i IT-tjänsteleverantörens eller apparatleverantörens system.

Under det gångna året lyftes även företagens och organisationernas strategiska samarbetspartner fram på motsvarande sätt. Beroendeförhållandena med sådana företag är tätare och partnerskap kan inte ersättas så lätt.

Som en del av attackerna utnyttjades också tjänster som är centrala för den digitala infrastrukturens och nätets funktion, bland annat namntjänster. Dessutom stod informationssäkerhetslösningarnas tillförlitlighet på spel när man försökte göra intrång i Virtual Private Network (VPN) -tjänster och -lösningar som användes för att skapa en säker nätverkskorridor.

Man kan även försöka utnyttja personers privata apparater för att göra intrång i enheter eller system som administreras av en organisation.

Även journalister, forskare och oliktänkande blir måltavlor

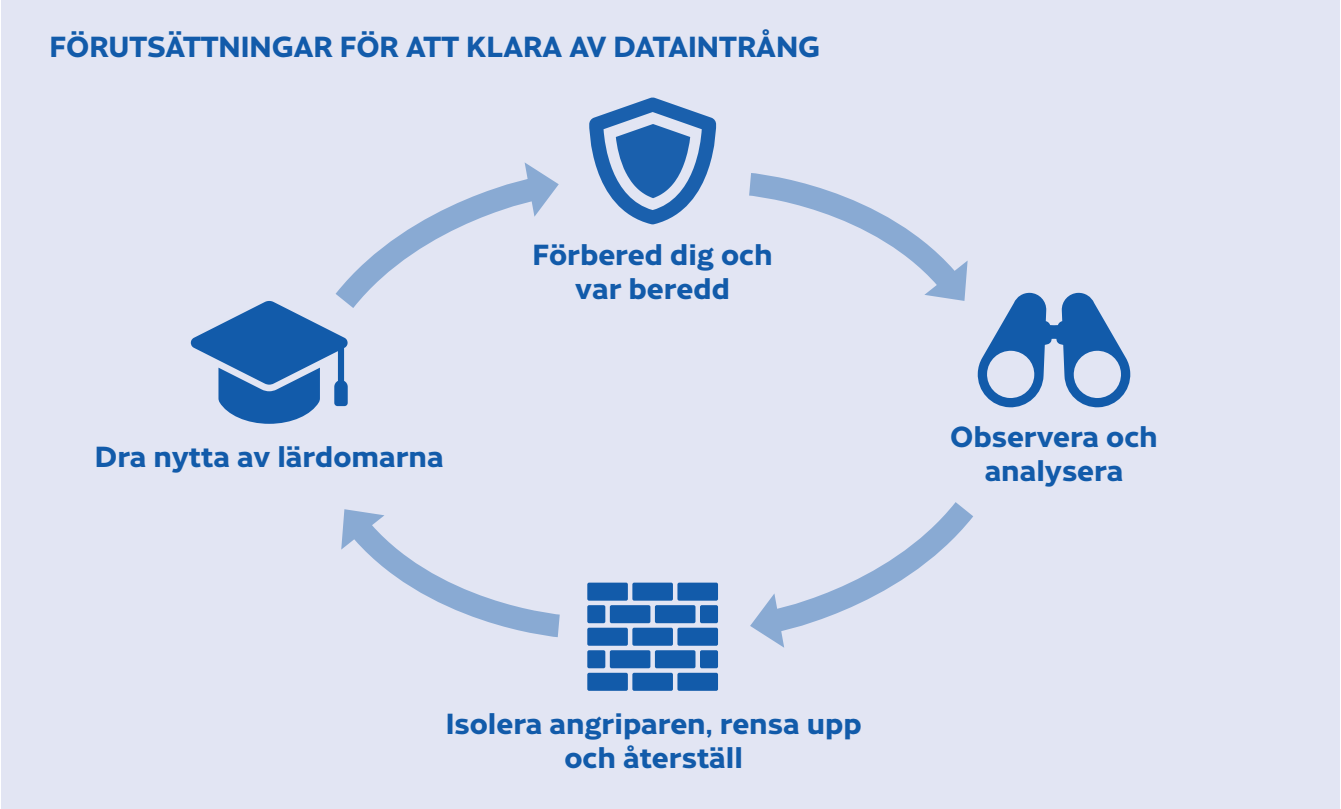
Under det gångna året spionerades det också på enskilda personer, folkgrupper och forskare. I flera nyheterinslag rapporterades det till exempel om Kinas försök att övervaka sin uiguriska minoritet.

Dessutom kan stater försöka spionera på eller övervaka sina medborgare som är bosatta utomlands, oliktänkande och aktivister eller journalister eller forskare som arbetar med dessa frågor. Sådana försök kan också påverka människor som bor i Finland eller organisationer som verkar här.

Beredskapsnivån varierar

I Finland har en del organisationer förberett sig betydligt bättre på hot om spionage än andra. Beredskapsbehovet gäller inte heller enbart verksamhet på inhemsk mark, utan man kan ibland av politiska skäl påverka västerländska företag med hjälp av cyberspionage.

Utöver tekniska lösningar bör beredskapen utvecklas genom ökad medvetenhet. Väldigt olika organisationer blir föremål för spionage på grund av sin egen verksamhet, den information de besitter eller sin ställning i leveranskedjan.



1 För två månader sedan skickades nätfiskemeddelanden som riktades till din organisation. Du får information om avsändaradressen.

- Kan du med dessa uppgifter hitta meddelandet och ta reda på vilka det har skickats till?
- Får du reda på om meddelandet har öppnats och om användaren har klickat på länken i meddelandet?

2 Du får information om kommandoservertrafiken för ett sabotageprogram som skickas från din organisation. Anmälaren informerar dig om tidsstämpeln och kommandoserverns domännamn.

- Kan du identifiera från vilken enhet trafiken kommer?
- Får du reda på vilket program eller vilken process som orsakade trafiken?
- Hur säkerställer du att eventuellt bevismaterial inte försvinner eller förstörs under processen då avvikelser hanteras?

3 Vi försöker nå den person i er organisation som ansvarar för informationssäkerheten för att utreda eventuella iakttagelser i anslutning till den statliga verksamheten.

- Har er organisation definierat ansvaret i datasäkerhetsfrågor?
- Kan våra experter hitta kontaktuppgifterna till er datasäkerhetsansvarige eller kontakta honom eller henne på annat sätt?
- Vet du var du kan få hjälp med den fortsatta utredningen av ärendet?

Skadliga program och sårbarheter

År 2019 kommer man ihåg att snabbt utnyttja nya sårbarheter. Tiden från publiceringen av sårbarheten till utnyttjandet av den förkortades avsevärt jämfört med tidigare. Organisationerna bör i sina informationssäkerhetsprocesser förbereda sig särskilt på att snabbt installera kritiska uppdateringar eller på att snabbt ta i bruk andra bekämpningsmetoder. Det är skäl att i synnerhet ständigt hålla system som är öppna på internet uppdaterade. Kritiska uppdateringar eller andra begränsningsmetoder bör tas i bruk genast och inte först vid nästa serviceavbrott.

Exim-sårbarheten utnyttjades mycket snabbt vid dataintrång

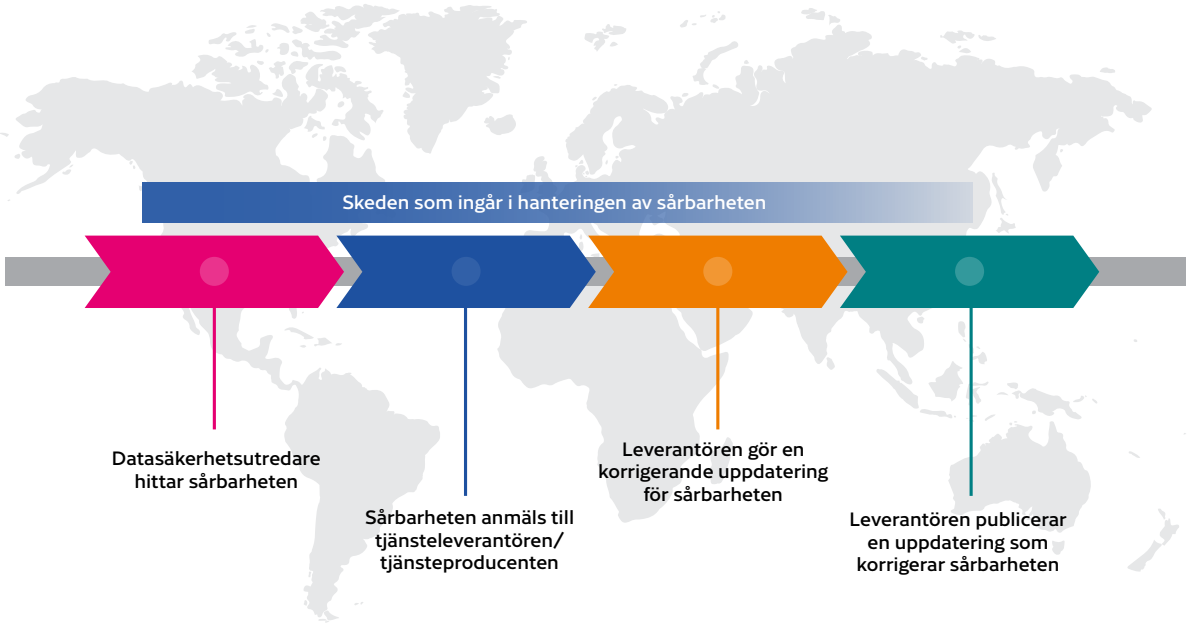
Av e-postserverprogrammet Exim publicerades en sårbarhet som möjliggjorde distansanvändning torsdagen den 6 juni 2019. Genast följande veckoslut genomfördes ett flertal dataintrång i Finland med hjälp av sårbarheten. Därför varnade vi måndagen den 10 juni för att Exim-sårbarheten utnyttjas.

Massutnyttjandet av sårbarheten börjar inte nödvändigtvis genast. Till exempel offentliggjordes den så kallade BlueKeep-sårbarheten i anslutning till olovlig distansanvändning i Microsoft Windows RDP-fjärrhanteringstjänst i maj 2019. Det tog flera månader innan det fanns en offentlig metod för att utnyttja sårbarheten (exploit). Dessförinnan hade sårbarheten utnyttjats i enskilda fall. När sårbarheten offentliggörs är det svårt att förutse hur snabbt det blir ett verktyg för brottslingar.

En del av de enheter som är anslutna till internet underhålls inte alls eller mycket sällan

För få internetuppkopplade apparater underhålls. Detta blev tydligt när vi bland annat utredde följderna av BlueKeep-sårbarheten i Finland. I slutet av maj skannade vi in Finlands internetadresser och hittade 414 sårbara system kopplade till internet. Vi kontaktade ägarna till dessa enheter via teleföretagen. Nästan två veckor senare fann vi fortfarande 353 sårbara system, vilket innebär att antalet bara hade sjunkit med cirka 15 procent. System som är anslutna till nätet och sårbara söker även brottslingar efter.

Tidslinje för nolldagssårbarhet



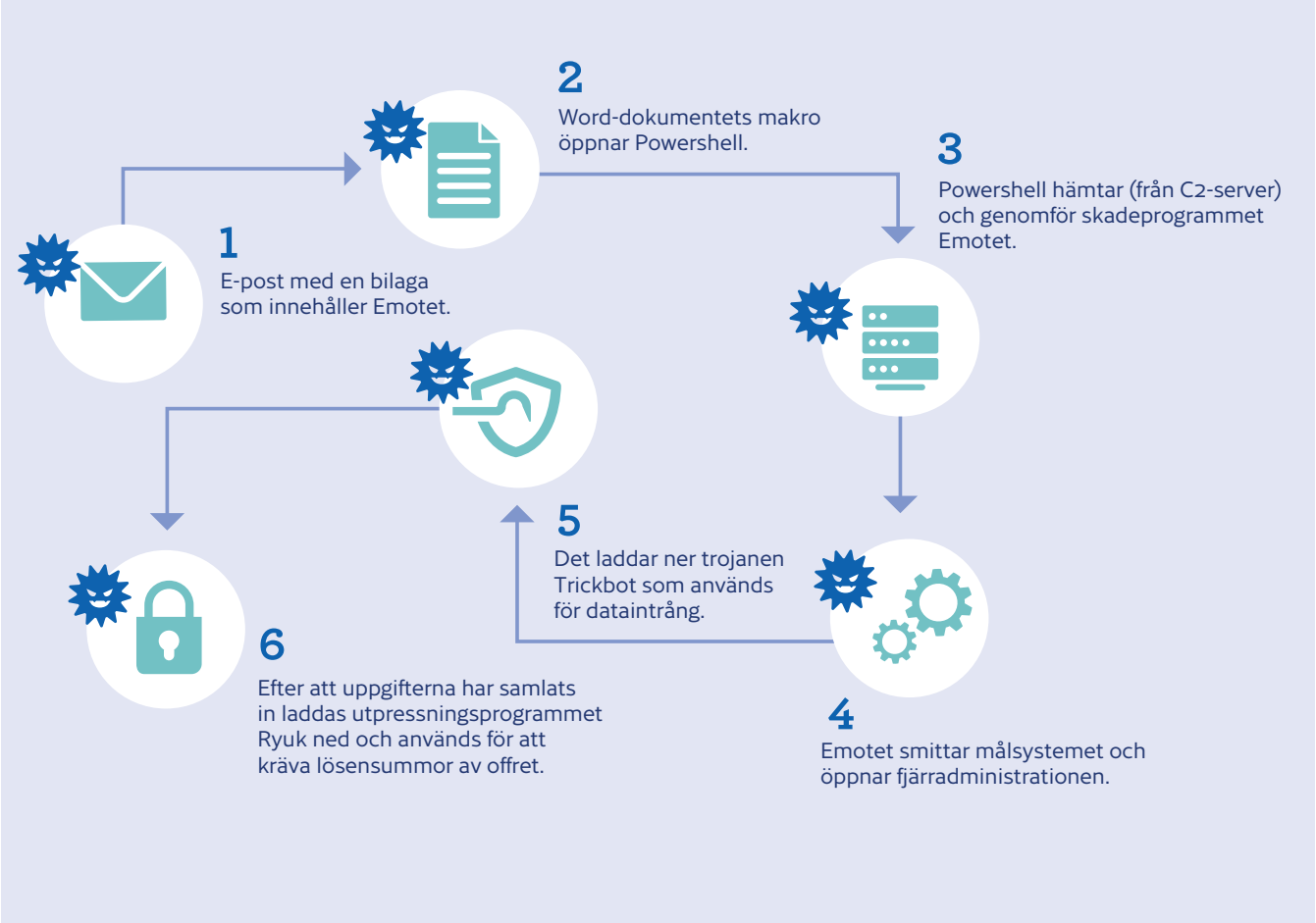
En omfattande utpressningsattack kan kosta tiotals miljoner

Omfattande attacker med utpressningsprogram under det gångna året Diskuterades mycket. Kriminella grupper som gjort framsteg i fenomenet big game hunting jagar företag eller organisationer vars verksamhet skulle påverkas avsevärt av det vida spridda utpressningsprogrammet.

Kriminella grupper har specialiserat sig på olika delområden av cyberbrottslighet och säljer sina tjänster vidare till varandra

En grupp koncentrerar sig på att sprida skade program i så stor omfattning som möjligt, till exempel genom att använda stulna e-postkedjor, som peppras med skadliga bilagor. En annan grupp samlar in information med hjälp av skadeprogram, till exempel lösenord och kreditkortsnummer, och klassificerar dem för återförsäljning. En tredje köper tillträde till de mest lämpade objekten och installerar ett utpressningsprogram som krypterar objektets hela datanätets servrar, nätverksdiskar och viktigaste arbetsstationer. Samtidigt lamslås objektets verksamhet. För att frigöra uppgifterna krävs offret på en lösensumma på tiotusentals eller hundratusentals euro. Samtidigt lamslås objektets verksamhet.

Så här framskrider attackkedjan för skadliga program i samband med big game hunting:



Svårt att upptäcka trovärdiga bedrägerimeddelanden

Den kriminella grupp som sprider skadeprogrammet Emotet har utvecklat ett effektivt sätt att lura mottagare med e-postmeddelanden.

E-postmeddelandekedjorna för den som blivit offer för ett dataintrång stjäls och skickas vidare till offrets adressbok med en bilaga som innehåller skadeprogrammet. Innehållet i meddelandet har alltså lånats från en äkta diskussion, vilket kan göra det svårt att identifiera det som skadligt. Sabotageprogrammet sprider sig alltså kedjemässigt från ett offer till ett annat genom att utnyttja ett befintligt förtroende. De skadliga meddelanden som bildats på detta sätt påminner till sin trovärdighet rentav om riktade meddelanden som skickats av statliga aktörer (spearphishing).

Hotet mot organisationer allt allvarligare

I Europa har exempelvis den danska tillverkaren av hälsoteknologi Demant, det norska aluminiumbolaget Norsk Hydro, den tyska tillverkaren av automationsteknologi Pilz, den franska tv-kanalen M6 och den spanska mediekoncernen Prisa fallit offer för big game hunting.

Kostnaderna är betydande när det är fråga om utpressningsprogram. Enligt deras egen rapportering drabbades till exempel Norsk Hydro under första halvåret 2019 av en totalkostnad på 55–65 miljoner euro. Demant å sin sida uppskattar att kostnaderna är ännu större, till och med närmare hundra miljoner dollar.

Den som attackerar försvårar medvetet återhämtningen

När en kriminell grupp får fotfäste i en organisation försöker den obemärkt sprida sig så mycket som möjligt i målorganisationen. En sådan attack har organisationen mycket svårt att återhämta sig från med sedvanliga medel. Efter att det skadliga programmet har startats krypteras uppgifterna med stark kryptering, som det ofta är omöjligt att häva med de nuvarande verktygen.

Brottslingar försvårar också vanligen återhämtningen efter attacken till exempel genom att kryptera filer och system samt säkerhetskopior och uppgifter om den centraliserade hanteringen av användarrättigheter. Därefter kräver den som utför attacken en betydande lösensumma i utbyte mot att lämna ut krypteringsnyckeln. I de fall som tagits upp i offentligheten har kraven på lösensumma varit till och med över en halv miljon euro.

Det finns flera metoder för att göra intrång och sprida ut sig i en organisations system. I skyddet betonas en övergripande hantering av datasäkerheten och tryggande av dess grundläggande nivå inom alla delområden.

Om en angripare ändå får in en fot är det mycket viktigt att organisationen kan upptäcka ovanliga händelser och spridningsförsök innan krypteringen börjar.

Ibland räcker det inte heller, utan angriparen går vidare till krypteringsfasen. Då hjälper bland annat inövade återställningsmetoder och sådana säkerhetskopior som kan tas i bruk även vid omfattande störningar. Dessa kopior ska vara skyddade så att angriparen inte har möjlighet att komma åt dem, även om han eller hon hade väntat på ett lämpligt tillfälle i systemen.

Utbetalning av lösensummor uppmuntrar till att söka fler offer

Det är svårt att på förhand definiera sannolika offer. Världen har sett tecken på att brottslingar i synnerhet är intresserade av stora och betalningsdugliga företag samt organisationer vars produktion kan störas avsevärt med hjälp av ett utpressningsprogram. Även regionförvaltningen samt kommun- och hälsovårdssektorn har varit i skottlinjen.

Det är också omöjligt att säga om fallen med utpressningsprogram blir vanligare i Finland. Så länge angriparna inte får lösensummorna, signalerar man till dem att cyberbrottslighet inte lönar sig. Då blir Finland inte heller ett objekt som lockar angripare. Om det däremot blir vanligare att lösensummor betalas ut, är det nästan säkert att brottslingarna konstaterar att de har en chans.

CHECKLISTA

FÖREBYGG OCH VAR BEREDD

- Sköt om det grundläggande dataskyddet.
- Säkerhetskopiera så att säkerhetskopiorna kan återställas även vid utpressning.
- Observera hot i riskbedömningen.
- Gör en handlingsplan för krissituationer och var beredd på kommunikationsbehov.
- Öva på att återställa säkerhetskopior.
- Testa er observationsförmåga.

UPPTÄCK I TID

- Ta i bruk omfattande loggning.
- Försök observera spridning i organisationens nätverk.
- Identifiera ledningskanalerna.
- Upptäck olovlig användning av användar-namn eller att nya huvudanvändarnamn skapas.
- Utnyttja informationssäkerhetsegenskaperna hos de lösningar och system ni redan har.

SÄKERSTÄLL ÅTERHÄMTNING

- Se till att säkerhetskopior finns tillgängliga även i störningssituationer.
- Säkra den centraliserade hanteringen av användarrättigheter.
- Säkerställ att säkerhetskopiorna är rena.
- Anmäl attacken till myndigheterna. Cybersäkerhetscentret erbjuder hjälp vid kränkning av informationssäkerheten. Gör även en polisanmälan.

Dataintrång och dataläckor

Bland det som hände i fjol sticker fortfarande dataintrången via Office 365 ut. Intrång i Office 365 sker huvudsakligen med hjälp av nätfiskade koder. Genom dataintrång strävar man efter att få tillgång till konfidentiellt material, göra faktureringsbedrägerier med uppgifter som man fått i sin besittning eller göra nya dataintrång med hjälp av de användarnamn och lösenord man fått tag på.

> ”Under sommaren drabbades flera finländska kommuner av dataintrång. Kommunsektorns dataintrång och cybersäkerhetsläget behandlas i en separat artikel på sidan 34.

Kommunernas dataintrång sommaren 2019

Under våren blev det allt vanligare med ett fenomen där cyberbrottslingar sökte stora företag eller organisationer inom den offentliga förvaltningen vars verksamhet de kunde störa i ett försök att pressa dem på stora summor pengar. Big game hunting har orsakat betydande förluster för de organisationer som blivit utsatta. Mer information om ämnet finns på sidan 34.

Oklar ansvarsfördelning orsakar dataintrång

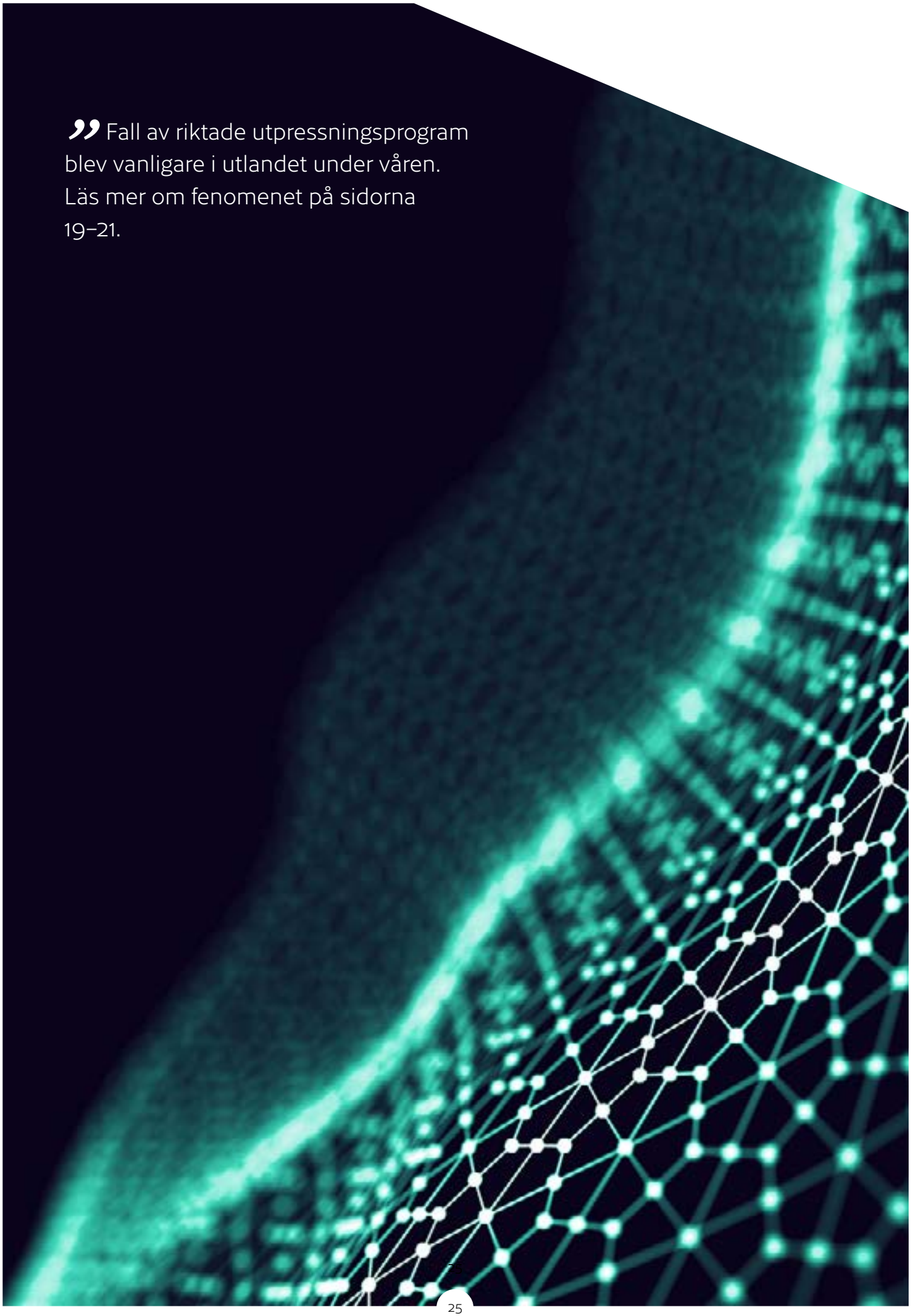
Vid planeringen av utlokaliseringar och serviceavtal är det skäl att beakta ansvaret för underhållet och uppdateringen av systemen och programmen. Under det gångna året har vi fått kännedom om flera dataintrång som berott på att system eller enheter inte är uppdaterade och där underhållsansvaret har varit oklart. I en miljö med många aktörer är det skäl att i förväg fastställa ansvar och om rätten att stänga system och till exempel behandla loggar. Gemensamma övningar med tjänsteleverantörer är i allmänhet ett bra sätt att gå igenom ansvar vid underhåll och i problemsituationer.

Anvisningar och gemensamma förfaringssätt för anställda förhindrar informationsläckage

Behandlingen av uppgifter som ska skyddas till exempel i offentliga molntjänster kan medföra en risk för dataläckor. Likaså är det skäl att ge anvisningar om verksamheten till exempel under arbetsresor så att information som ska skyddas åtminstone inte lätt hamnar i fel händer. Tyvärr kan avsaknaden av egna lösningar eller verksamhetssätt i organisationen eller att de inte fungerar orsaka situationer där det lättaste tillvägagångssättet medför en risk för dataläckor.

Dataintrång är ett brott

Ju fler anmälningar vi får om dataintrång och informationsläckage, desto bättre kan vi skapa en lägesbild av cybersäkerheten och även hjälpa andra som faller offer för dataintrång. Det är bra att komma ihåg att ett dataintrång eller försök till det är ett brott, så vi rekommenderar att man polisanmäler dataintrång. Kom ihåg att dataombudsmannen ska underrättas om personuppgifter kommer i fel händer i samband med en dataläcka.



”Fall av riktade utpressningsprogram blev vanligare i utlandet under våren. Läs mer om fenomenet på sidorna 19–21.

Nätfiske och bedrägerier

Nätfiske efter användarnamn och lösenord färgade 2019. Bluffmeddelanden ledde sina mottagare till olika webbplatser avsedda för nätfiske. Förevändningarna var många: godkänn de nya användningsvillkoren för din bank enligt direktivet; öppna en fil som din kollega delat i det interna nätet; logga in på nytt i tjänsten; bekräfta din inloggning i molntjänsten eller kontot på sociala medier. Inte i ett enda fall var länken som kom med meddelandet äkta, utan skickad av en bedragare. På så sätt hamnade bankkoderna och lösenorden som matats in på nätfiskesidorna hos bedragare för som använde dem för dataintrång. År 2019 var fallen beklagligt vardagliga.

Nätfiske och -intrång via Office 365 är redan vardag

Redan i juni 2018 publicerade vi en varning för nätfiske av användarnamn och lösenord till Office 365. Varningen hann vara i kraft i över ett år tills vi till sist tog bort den 16 september 2019. Fenomenet har dock inte minskat eller helt försvunnit, eftersom Office 365 -användarnamn fortfarande hamnar i brottslingars händer dagligen. På hösten tog vi bort vi varningen eftersom anmälningarna om nya fall hade lugnat ner sig. Hotet om nätfiske och dataintrång har dock inte minskat, utan vi får fortfarande nästan varje dag anmälningar om intrång i Office 365. Dessutom har användningen av användaruppgifter som fåtts genom nätfiske vid dataintrång blivit snabbare under det gångna året och trenden förväntas fortsätta.

Sommaren 2019 publicerade vi en guide om skydd mot nätfiske och dataintrång i Microsoft Office 365. Guiden finns på finska och engelska på vår webbplats. Skyddet underlättas i synnerhet av att man inför autentisering i flera faser, vilket om det görs korrekt hjälper till att bekämpa utnyttjandet av användaruppgifter som hamnat i fel händer. Enligt Microsoft skulle nästan alla intrång i Office 365 kunna förhindras genom tvåfaktorsautentisering. Tyvärr ser det ut som om dataintrången via Office 365 kommer att fortsätta även under 2020. Vi rekommenderar att man till Office 365-miljön, liksom för upprätthållandet av andra molnlösningar använder separata underhållskoder, varvid det orsakar mindre olägenhet för hela molnlösningen om användaruppgifter hamnar i fel händer.

Bild av faserna i Office 365

Hackade e-postkonton används för bedrägeri

År 2019 förekom också vd-bedrägerier och andra faktureringsbedrägerier. Flödet av falska e-postmeddelanden och förfalskade snabbmeddelanden sinade aldrig. Bluffmeddelanden skickades också från hackade e-postkonton och konton på sociala medier. Det som i Finland kallas vd-bedrägerier är bedrägerier där man närmar sig den som ansvarar för organisationens betalningsrörelse och utger sig för att vara direktör och per personen betala en avgift snabbt, vanligen till ett utländskt konto. Bedragaren åberopar brådska och konfidentialitet, påstår sig befinna sig i en situation där kommunikationen fungerar dåligt och kräver snabba åtgärder.

Utöver företag har alla slags organisationer från idrottsföreningar och bibliotek till sjukhus och församlingar blivit föremål för vd-bedrägerier. Det är lätt att förfalska sådana meddelanden per e-post för att se ut som skickade av en riktig direktör, men även andra kommunikationskanaler används. Nya trick för 2019 har varit att begära om ändring av lönekonton till bedragarnas konto, köp av presentkort till olika webbtjänster och att skicka koder till bedragare. Särskilt för köp av presentkort som affärsgåva är lämpligt för ljusskygg verksamhet och hjälper bedragaren att bedra på ett trovärdigt sätt.

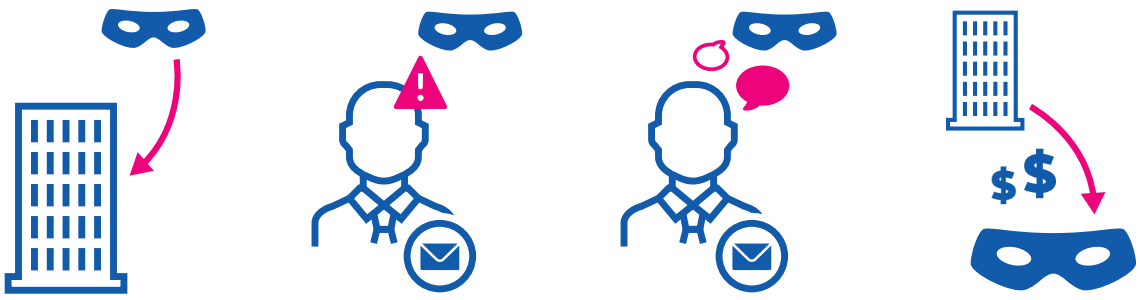
Man kan inte lita på textmeddelanden

Textmeddelandenas andel av alla bedrägerier fortsatte öka 2019. Bland annat abonnemangsfällor, placerings- och penningtvättsbedrägerier plingade till just som textmeddelanden i mobila enheter. Vi har redan lärt oss att betrakta e-post som en kanal för bedragare, men textmeddelanden har ännu inte samma rykte. Denna uppfattning kunde bedragarna utnyttja. Ett textmeddelande som lästs med en smarttelefon för via länkar till opålitliga sidor för nätfiske och bedrägeri, precis som e-post.

De största bedrägerikampanjerna via textmeddelande sågs redan i början av året och under våren i Postis namn. En ankomstavi som förfalskats i Postis namn syntes i mottagarens telefon i samma meddelandekedja som riktiga textmeddelanden från Posten, och därför verkade de trovärdiga. Det lönar sig dock att misstänka lurendrejeri om "Postens" länk i stället för ett paketmeddelande öppnar en sida om en tävling, utlottning och en möjlighet att för en euro köpa underhållningsutrustning värd hundratals euro.

Förutom beställningsfällor och bedrägerier användes textmeddelanden också för att fiska bankkoder och för att förbigå stark autentisering.

Det finns många sätt att hamna i abonnemangsfällor: reklam, bedrägeri, meddelanden på sociala medier, textmeddelanden, webbsökningar, kedjebrev. Förevändningen kan vara en utlottning, tävling, förfrågan, ankomstavi eller ett annat meddelande, men slutresultatet är oftast detsamma: den bedragna tror sig ha deltagit i en tävling och vunnit ett pris, till exempel en telefon eller TV för en euro, men i den finstilta texten står det att konsumenten har förbundit sig till en månadsavgift för en onödig tjänst. Den bedragna blir utan sitt pris, men bedragaren som fått kreditkortsnumret får 80 euro varje månad.



1. Sökning av objekt **2.** Bygga upp förtroende **3.** Informationsutbyte **4.**Transaktion

BEC – Business Email Compromise eller faktureringsbedrägeri.

UPPTÄCKTA BEDRÄGERIER I FINLAND 2019

EXEMPEL PÅ UTPRESSNING

- **Porrutpressning:**
  E-postmeddelande där bedragaren påstår sig ha hackat offrets dator och installerat ett spionprogram som har spelat in när offret till exempel har tittat på vuxenunderhållning. Bedragaren kräver lösen för att inte offentliggöra en känslig upptagning. Ibland försöker man göra utpressningen mer trovärdig med hjälp av något gammalt lösenord: "Jag kan ditt lösenord, så det är säkert att jag talar sanning."

- **Dödshotsutpressning:**
  Bedragaren påstår sig vara en lönnmördare som anlitats för att mörda sitt offer. Men även här skulle offret klara sig undan genom at betala stora lösesummor.

- **Skräppostutpressning:**
  Utpressaren hotar att förstöra företagets rykte genom att inleda en enorm skräppostkampanj i företagets namn, om inte lösensummorna betalas.

- **Utpressning med överbelastningsangrepp:**
  Utpressaren hotar att slå ut företagets datanät med hjälp av överbelastning om företaget inte betalar lösen. Ibland kan dessa hot vara förknippade med ett litet prov från en överbelastningsangrepp som nätbrottslingar utför gratis.

EXEMPEL PÅ FAKTURERINGSBEDRÄGERIER

- **Vd-bedrägeri:**
  Bedragaren låtsas vara direktör och närmar sig den som har hand om organisationens pengar via e-post, via sociala medier eller någon annan kanal. Syftet är att få till stånd en transaktion med hjälp av en förevändning till ett konto som bedragaren använder.

- **Lönebetalningsbedrägeri:**
  Bedragaren låsas vara direktör och ber organisationens löneräknare att ändra ett lönekonto till ett av bedragarens konton.

- **Presentkortsbedrägeri:**
  Bedragaren låtsas vara direktör och begär att presentkort snabbt ska ordnas. Koderna på presentkorten kan bedragaren förvandla till pengar.

Sakernas internet

Sakernas internet, som tidigare ansågs vara ett framtidsfenomen, är nu vår vardag. Smarta enheter har blivit bekanta för oss till exempel genom olika underhållningstjänster, idrottsevenemang och hemteknologi. Tjänster kan också produceras på platser där det inte tidigare var möjligt. Sådana tjänster är bland annat mjuka leksaker avsedda för att övervaka barn, som innehåller övervakningsmöjligheter på avstånd eller apparater som fungerar med röstkommandon och som används för att styra hemmet. Sårbarheter i apparaterna kan göra det möjligt för utomstående att få tillgång till både video- och ljudmaterial.

Apparater som ansluts till internet är fortfarande sårbara. Säkerheten hos inbyggda program förbättrades inte heller 2019. En omfattande undersökning genomförd av datasäkerhetsföretaget Cyber ITL (https://cyber-itl.org/2019/08/26/iot-data-writeup.html) visade att Internet of Things, det vill säga tillverkare av IoT-produkter, år efter år upprepar samma fel i sina produkter och att ingen utveckling skett på över tio år.

Oskyddade IoT-apparater även hos oss

Vi ser många IoT-apparater som ligger öppet på Internet och är sårbara även i Finland. Utrustning som innehåller brister i informationssäkerheten kan till exempel användas i botnät för att effektivisera överbelastningsangrepp. Till exempel har IoT-enheterna fått Mirai-bot-nätet att växa särskilt mycket 2019. Ett beklagligt faktum är att spridningen av sakernas internet även ger brottslingarna nya förtjänstmöjligheter.

Tills vidare har IoT-apparaternas datasäkerhetsnivå varit låg. Lyckligtvis har behovet av internationella IoT-standarder uppstått både i Europa och USA. Slutet av 2019 gav konsumenterna och företagen lättnad i form av exempelvis reglering och cybersäkerhetsmärket. Vi hoppas att de hjälper så många konsumenter som möjligt med deras köpbeslut.

Kom ihåg att testa! Bättre IoT redan i produktutvecklingsfasen

IoT har medfört fördelar, men även informationssäkerhetsutmaningar. Dessa utmaningar måste åtgärdas innan en IoT-apparat ansluts till internet.

Utmaningarna varierar beroende på apparat. Till exempel låsning av apparater i hemmet medför betydande säkerhetsutmaningar. Man svarar bäst på utmaningarna när man tar med datasäkerhetsegenskaperna redan i planerings- och utvecklingsfasen.

Bedömningen av helhetssituationen och utmaningarna kräver mer forskning. Ändå kan vi konstatera att man får mest ut av fördelarna med IoT-tekniken om grunderna har skötts väl. Ett säkert sakernas internet bygger på en trygg programvaruutveckling inom teknologierna, noggrann testning och regelbundna uppdateringar. Tjänster som produceras med hjälp av IoT-apparater medför utmaningarna men också många möjligheter.

Centrala informationssäkerhetsrisker för privatpersoner, organisationer och statsförvaltningen

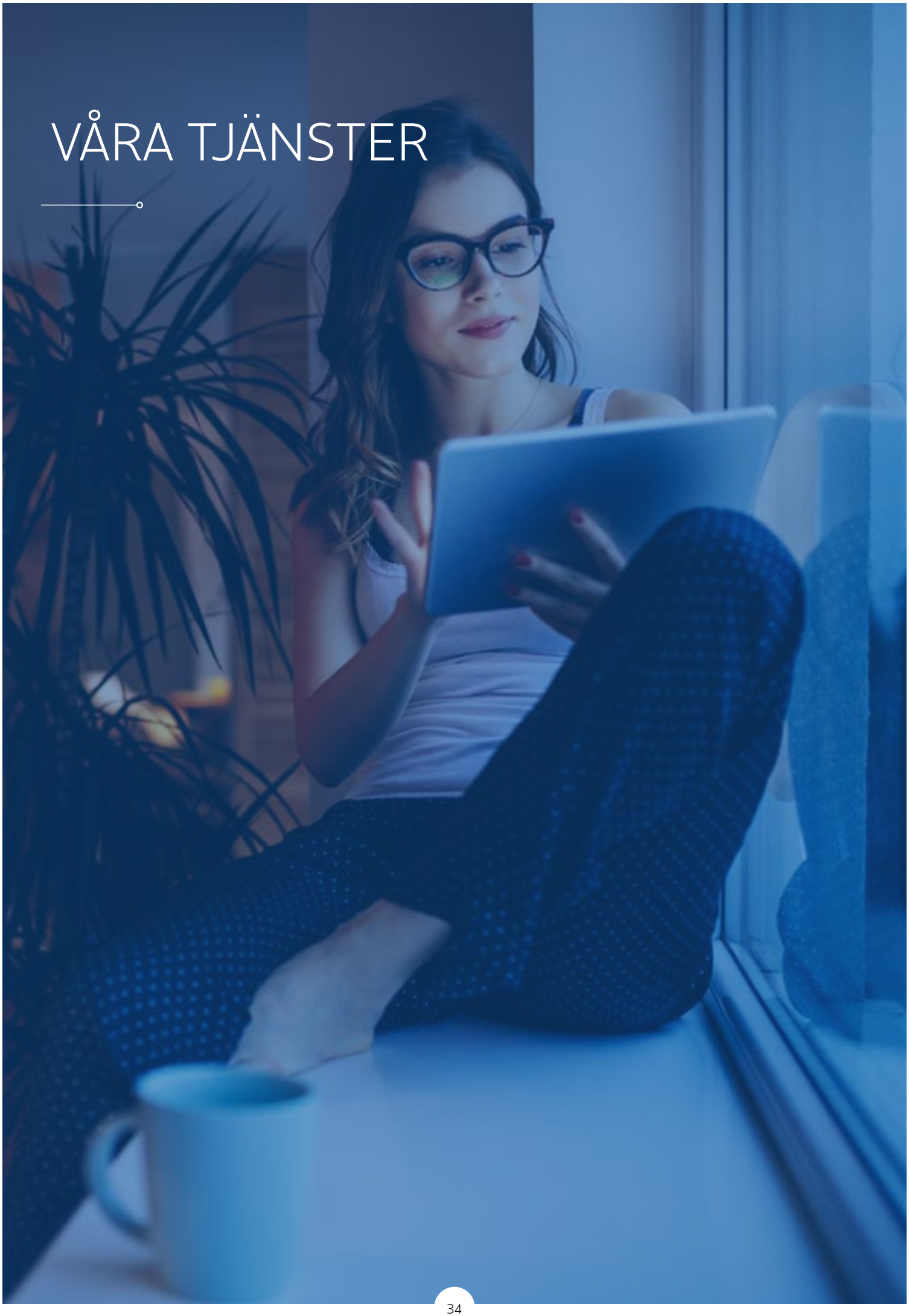
Här bedömer vi de största riskerna i anslutning till stora cybersäkerhetsfenomenen 2019. Vi har lyft fram exempelfall på hur riskerna har kunnat se ut för privatpersoner, företag, kommunala organisationer eller statsförvaltningen.

Pilens riktning berättar hur situationen har utvecklats jämfört med 2018. Vår uppfattning är att den allmänna risknivån för cybersäkerheten i Finland 2019 hölls så gott som oförändrad jämfört med år 2018. Riskerna har inte minskat, snarare har de förblivit oförändrade eller blivit allvarligare.

= Risken har förblivit densamma ▲ Förhöjd risk

KOMMUNIKATIONS-NÄTENS VERKSAMHET	= Användningen av digitala tjänster ökar, men man är inte djupt beroende av att de fungerar.	= Allt fler organisationer har förberett sig på störningar i ICT-tjänsternas funktion. Reservåtgärderna är dock inte alltid tillräckliga.	▲ Underhållet av de gamla ICT-systemen tar resurser från de gemensamma systemens funktionssäkerhet, underhåll och utveckling.
ÖVERBELAST-NINGSANGREPP	= Hackade routrar och andra IoT-apparater i hemmet används fortfarande som en källa till överbelastningsangrepp.	= Beredskap för överbelastningsangrepp bör beaktas när en organisation planerar och skaffar webbtjänster.	= Offentliga tjänster är tyvärr ett populärt mål för överbelastningsangrepp. I synnerhet de kritiska tjänsternas funktion bör garanteras i alla situationer.
SPIONAGE OCH PÅVERKAN	= Sannolikheten att finländska privatpersoner ska bli föremål för spionage är i huvudsak oförändrad. Oliktänkande med anknytning till auktoritära länder och inflytelserika politiska personer löper risk att bli föremål för spionage.	▲ Företag utsätts för spionage av både ekonomiska och politiska intressen. Genom att störa organisationernas verksamhet kan man också sträva efter att påverka samhället.	= Fortfarande ett centralt mål för spionage. Med hjälp av spionage gynnas den egna politiska ställningen, man inhämtar information om beslutsfattande, bedömer beredskap och skicklighet samt förberedelse för annan oönskad påverkan.
SKADLIGA PROGRAM OCH SÅRBARHETER	= Sårbara IoT-apparater infekteras snabbt med skadliga program. Programmen uppdateras alt oftare automatiskt.	= Sårbara apparater uppkopplade till internet letas upp och hackas snabbt. Även sårbarheter hos automatutrustning har utnyttjats.	▲ I synnerhet hantering av sårbarheter och vikten av underhåll har betonats.
DATAINTRÅNG OCH DATALÄCKOR	= Risken för dataintrång var nästan densamma för ett år sedan. Antalet stora läckor med användaruppgifter har ökat.	▲ Fallen med utpressningsprogram har blivit vanligare. Dessutom har i synnerhet antalet dataintrång via O365 ökat.	▲ Statsförvaltningen berörs av samma hot och risker som organisationerna. Antalet dataintrång och dataläckage har ökat.
NÄTFISKE OCH BEDRÄGERIER	▲ Medborgare utsätts för allt skickligare bedrägerier. Utpressningsbedrägerier, bankfiske och abonnemangsfällor blir allt svårare att bekämpa.	▲ Kanske har man ännu inte sett toppen av nätfisket på företagskonton, tyvärr.	= Vd- och faktureringsbedrägerier är också vardag inom statsförvaltningen, men man förstår riskerna bättre än tidigare.
SAKERNAS INTERNET	= Säkerheten hos program för konsumentprodukter har inte utvecklats på flera år. Cybersäkerhetsmärket och den utvecklande standardiseringen stöder valet av säkra apparater.	▲ Säkerheten hos inbyggda program har inte utvecklats på flera år.	= Utmaningarna förblir oförändrade, inga helt nya omfattande risker har uppstått.

VÅRA TJÄNSTER



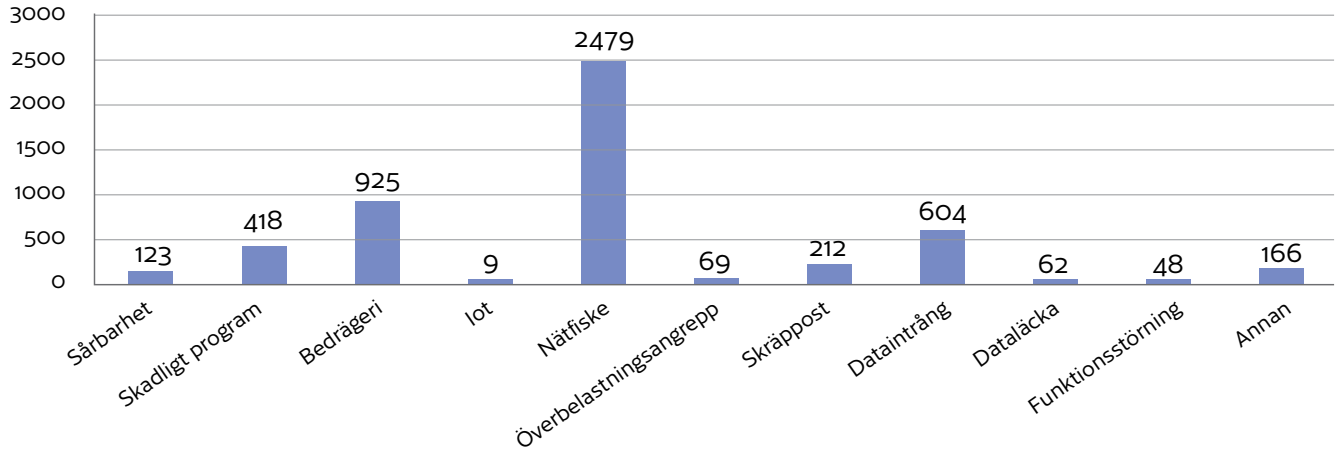
På lägescentralen behandlas tusentals fall per år

På vår lägescentral ger vi dagligen råd och stöd till ett stort antal offer för kränkningar av informationssäkerheten. Den som behöver hjälp kan vara en enskild medborgare, men också ett storföretag eller en kommun. Våra tjänster är kända under den engelska termen incident response (IR).

Hur allvarliga kränkningarna av informationssäkerheten är bedöms av två personer. Ofta kan hjälp ges redan under den första kontakten. Fall som kräver noggrann teknisk analys eller långvarig samordning förs vidare till mer detaljerad granskning.

Med Lahtis och Kumo höll vi regelbundna lägesmöten där vi redde ut vad som händer, hurdana återhämtnings- eller skyddsåtgärder som har vidtagits och vilka fortsatta åtgärder som var under planering härnäst.

Snabba – i bästa fall även inövade – handlingssätt och kännedom om den egna miljön och systemen hjälper om en attack drabbar en själv.



År 2019 behandlade vår situationscentral cirka 4 500 fall. I antalet fall syns inte de fall som automatiskt behandlas i vårt Autoreporter-system.

Varje år behandlar vi tusentals fall. Antalet fall av dataintrång ökade i synnerhet med Office 365-fallen. Dessutom har olika bedrägerier, bland annat abonnemangsfällor som skickats per e-post och textmeddelande varit ett problem i år.

Våra mest oförglömliga kunder under året var kommunerna Kumo, Björneborg och Lahtis. De fick uppleva vad det innebär att bli föremål för en cyberattack.

I alla fall anmälde städerna händelserna snabbt till vår lägescentral, genast när de upptäckt situationen. På så sätt kunde vi stödja och ge råd till offren för cyberattacken på bästa möjliga sätt.

Kommunerna har en viktig roll som producent av vardagliga funktioner och som kommuninvånarnas trygghet

När kommunernas tjänster fungerar fäster man inte desto större uppmärksamhet vid saken. Kommunerna har många olika tjänster som de ska upprätthålla. Under 2019 utsattes flera finländska kommuner för cyberattacker och kommunernas cybersäkerhet blev föremål för diskussion.

Kommunernas cybersäkerhetsnivå varierar och de tillgängliga resurserna, såväl de ekonomiska som de personalrelaterade, varierar väldigt mycket.

En cyberattack rubbar fortfarande hälso- och sjukvårdstjänsterna i Lahtis - CKP: "Vi gör allt för att fånga den som sprider denna ondska” YLE:s nyheter 13.6.2019

”Utpressarna kräver lösen från Kumo stad – sabotageprogram fick stadens nät på knä”

YLE:s nyheter 30.7.2019

"Återigen dataintrång i Satakunta: Denna gång utsattes Björneborgs stad”

YLE:s nyheter 8.8.2019

Ofta är problemet att det inte satsas tillräckligt på cybersäkerheten. Tjänsterna genomförs förmånligt och så att upprätthållandet av dem inte planeras. Dessutom genomförs underhållet av resursskäl enkelt, vilket kan betyda till exempel att det finns flera olika servicehelheter i ett och samma nät. Genom att angripa nätet en gång kan man få omfattande effekter.

Cybersommaren i Kumo, Lahtis och Björneborg var arbetsam

Attacken mot stadens datanät i Kumo orsakade omfattande olägenheter och störningar i ordnandet av stadens tjänster och funktioner. Till exempel fungerade inte stadens e-posttrafik och betaltransaktioner i och med attacken.

De direkta kostnaderna för attackerna mot stadens datanät i Lahtis hade vid årsskiftet redan stigit till cirka 900 000 euro. Även antalet indirekta kostnader uppskattas uppgå till hundratusentals euro, då nätanvändarnas arbetsuppgifter störddes av att nätet inte fungerade. Som försiktighetsåtgärd tvingades man bryta förbindelsen mellan Lahtis stad och Päijänne-Tavastlands välfärdssamkommun.

I Björneborg blev konsekvenserna av attacken lindrigare, men det fanns risk för större skada.

Under sommaren och hösten deltog vi i utredningen av cyberattackerna mot kommunerna i Björneborg, Lahtis och Kumo. Fallen förenades med omedelbara konsekvenser i synnerhet för ICT-tjänsterna. Kommunerna drabbades av ett dataintrång där man med hjälp av skadeprogram kom in i kom-

munens datanät. Angriparen valde inte nödvändigtvis just dessa kommuner som mål, snarare påträffade angriparen lätta offer, vars informationssäkerhetsnivå var låg. Då fick angriparen till stånd stora konsekvenser utan större besvär.

I det största kommunfallet tog sig angriparen in på nätet med hjälp av bristfällig åtskillnad av nätet och underhållsrättigheter varit i omfattande bruk. Å andra sidan reagerade det uppdaterade säkerhetsprogrammet på det som avvek från det vanliga i skadeprogram snabbt, och kommunens mycket sakkunniga tjänsteleverantör hindrade snabbt eventuella större skador. Ändå uppgick den totala kostnaden för cyberattacken till hundratusentals euro och effekterna var långvariga.

I övriga fall förhindrade väl genomförd åtskillnad av olika delar av nätet en bredare spridning av skadeprogrammet. Även säkerhetskopior gjorde det möjligt att återhämta sig snabbare.

På grund av det som hände under sommaren utredde vi nivån på kommunernas datasäkerhet. Enligt våra observationer finns det i kommunernas webbmiljöer många tjänster som är öppna på internet och som inte borde vara det. Sådana är till exempel oskyddad kontorsutrustning, apparater för hantering av nätverk, olika databasservrar och interna tjänster såsom hela intranätet. Föråldrade program och servrar orsakar också problem. Vi rapporterade våra observationer till kommunerna för att bristerna i informationssäkerheten skulle åtgärdas.

Samarbete och nätverk som en del av utvecklingen av kommunernas cybersäkerhet

Säkerhetskommittén gav hösten 2019 en rekommendation om förbättring av kommunernas cybersäkerhet: "Senaste tidens händelser har prövat kommunernas cybersäkerhet på olika sätt. Kommunerna ansvarar för åtgärderna och för att täcka kostnaderna, men Cybersäkerhetscentret vid Transport- och kommunikationsverket och andra myndigheter erbjuder kommunerna stöd med rådgivning och efterforskning."

För närvarande har Cybersäkerhetscentret ingen helhetsbild över cybersäkerheten i kommunerna eftersom det inte finns några avvikelser från anmälningsskyldigheten. En del av kommunerna gjorde en anmälan under 2019, vilket underlättade återhämtningen. Tillsammans med Kommunförbundet har vi konstaterat att det behövs ett eget nätverk för kommuner där man kan dela information. För detta ändamål har man inlett arbetet med att inrätta en samarbetsgrupp. Situationen förbättras avsevärt när kommunernas tillgänglighet underlättas och information kan fördelas målinriktat.

Datasäkerhetsreglering och -bedömningar

Ett superår för cybersäkerhets-lagstiftningen ligger bakom

År 2019 trädde flera lagar om informationssäkerhet och cybersäkerhet i kraft. Bland annat ändringarna i lagen om identifiering och betrodda tjänster medförde konkurrens i identifieringstjänsterna. När cybersäkerhetsförordningen trädde i kraft etablerades EU:s cybersäkerhetsbyrå ENISA:s ställning och det möjliggjorde inrättandet av ett europeiskt certifieringssystem för cybersäkerhet.

Dessutom fortsatte flera beredningsarbeten med anknytning till lagstiftningen. Till exempel förnyades innehållet i lagen om tjänster inom elektronisk kommunikation för att motsvara bestämmelserna i EU:s direktivpaket om elektronisk kommunikation. Även ePrivacy- eller dataskyddsförordningen bereddes inom EU.

Utöver lagprojekten under det gångna året övervakade vi och införde även lagstiftning som trätt i kraft tidigare.

Efterlängtad konkurrens på marknaden för identifieringstjänster

§

Ändringarna i lagen om identifiering och betrodda tjänster som trädde i kraft i början av året gav efterlängtad konkurrens på marknaden för starka elektroniska identifieringstjänster. Även de så kallade förmedlarna av identifieringstjänster inledde sin verksamhet. Vi uppnådde en situation där en leverantör av elektroniska tjänster kan konkurrensutsätta leverantörer av identifieringstjänster och vid behov få alla identifieringsverktyg för sina kunder genom att ingå ett avtal med en leverantör av förmedlingstjänster. Tidigare var man tvungen att ingå flera avtal. Genom att öka konkurrensen på marknaden sänks priserna för tjänsterna och användningen av stark autentisering i elektroniska tjänster främjas. Ju mer stark autentisering som används, desto säkrare blir vårt digitala samhälle.

TUPAS nådde vägs ände

§

TUPAS-protokollet som länge varit bekant för finländare från nätbanker och stark autentisering nådde sitt historiska slut. TUPAS, som utvecklades i Finland, var en progressiv lösning för stark autentisering. Man beslöt dock att slopa den, eftersom den inte längre uppfyllde moderna säkerhetskrav för stark autentisering. I stället infördes OIDC- och SAML-protokollen, som uppfyller de nuvarande kraven och som används mycket internationellt. Utvecklingen är en bra påminnelse om att system och tjänster ständigt måste utvecklas med tanke på både nuvarande och framtida säkerhetskrav.

Regionnätens funktionssäkerhet föremål för inspektion

Under de senaste åren har vi inspekterat i synnerhet de nya regionala näten och de aktörer som driver dem. Vårt mål har varit att säkerställa en tillräcklig funktionssäkerhet för näten och de tjänster som erbjuds på nätet genast efter ibruktagandet. Med regionnät avses tiotals lokala optiska fibernät som olika lokala aktörsgrupper har byggt för att erbjuda bredbandsförbindelser.

Vid inspektionerna går man igenom kommunikationsnätets funktion och säkerställandet av elförsörjningen, krav på jordning och störningshantering. Målet är att förbättra aktörernas medvetenhet om minimikraven och ge råd om utvecklingen av funktionssäkerheten. Utifrån inspektionerna kan man också åläggas att avhjälpa de brister som observerats. Även om inspektionerna alltid utförs av en enskild aktör samlar vi samtidigt in information om hur regleringen fungerar och om ändringsbehoven. Inspektionerna är också en viktig del av utvecklingen av regleringen av funktionssäkerheten och säkerheten i hela samhället.

Diskussion om cookies

Den så kallade Planet 49-lösningen, som Europeiska unionens domstol antog, ökade den offentliga debatten om cookies i kölvattnet efter den allmänna dataskyddsförordningen, GDPR. Tyvärr gav domstolens avgörande inga tydliga riktlinjer för fallen.

Enligt avgörandet krävs en aktiv åtgärd av användaren för samtycke till användning av cookies. Dessutom ska tjänsteleverantören ge information om hur länge cookies fungerar och om tredje part har möjlighet att använda dem. I domstolens avgörande behandlades dock inte om samtycke ska begäras till exempel via popupfönster. Det återstår att se om den dataskyddsförordning för elektronisk kommunikation som är under beredning medför förändringar i situationen.

System lämpade för skydd av internationell säkerhetsklassificerad information väldigt eftertraktade

Fenomenen i den nationella och internationella säkerhetspolitiken syntes också i våra utvärderingsobjekt, där man särskilt fokuserade på den internationella säkerhetsklassificeringens skydd av information. Vi utvärderar flera informationsbehandlingsmiljöer som är viktiga för samhällets funktion. Ägarna till säkerhetsklassificerad information hade fastställt ett nationellt myndighetsgodkännande som villkor för användningen av dem. Utöver databehandlingsmiljöerna godkände vi flera nya versioner av inhemska krypteringsprodukter.

Den allmänna stämningen vid NCSA under det gångna året var positiv när vi kunde stödja flera myndigheter och företag i behov av hantering av säkerhetsklassificerad information, behov som ställvis var mycket kritiska. För våra viktigaste utvärderingsobjekt under året kunde man bevilja myndighetsgodkännande. Utvecklingen av nationella och internationella fenomen lovar mycket intressanta utmaningar även för 2020!

En cookie är en liten textfil som webbläsaren sparar på användarens enhet. Med hjälp av cookies är det bland annat möjligt att samla in inköp i kundvagnen i en webbshopen innan de betalas. Bestämmelser om cookies finns i 205 § i lagen om tjänster inom elektronisk kommunikation. Det grundar sig på EU:s direktiv om dataskydd vid elektronisk kommunikation, som håller på att ersättas av en förordning.

Vår rådgivningstjänst har tagits emot väl – granskningstiderna blev snabbare

Liksom föregående år ökade behovet av informationssäkerhetsrådgivning. År 2019 behövdes stöd och anvisningar särskilt för att skydda den kritiska infrastrukturen i vårt samhälle samt för att skydda säkerhetsklassificerad information i datasystemen. Resultaten från vår rådgivningstjänst syntes i våra utvärderingsobjekt som bättre färdighetsgrader än tidigare, vilket bland annat påskyndade genomgångstiderna för inspektionerna.

Kriterier för bedömning av molntjänsters säkerhet

Redan länge har molntjänsternas informationssäkerhet väckt frågor både inom förvaltningen och i näringslivet. De kriterier som vi publicerade som stöd för utvärderingen av molntjänsternas säkerhet togs emot positivt.

Säkerhetskriterierna för molntjänster (PiTuKri) stöder myndigheterna i tillämpningen av den nya informationshanteringslagen. De innehåller också verktyg för att bedöma molntjänsternas säkerhet och risker i anslutning till dessa. Dessutom tar de upp god praxis som påverkar molntjänsternas säkerhet och som även kommersiella aktörer kan utnyttja.

Vi har fått mycket bra respons och utvecklingsförslag om kriterierna. I början av 2020 publicerar vi en ny version av dem som grundar sig på både respons och våra egna observationer.

De uppdaterade bedömningskriterierna stöder utvecklingen av identifieringstjänsternas säkerhet

Under 2019 uppdaterade vi bedömningskriterierna för stark autentisering utifrån erfarenheter från utvärderingsberättelser och informationssäkerhetsauditeringar. Kriterierna stöder leverantörer av identifieringstjänster och bedömare som utför auditeringar för dem för att utveckla och utvärdera tjänsternas säkerhet. Utifrån kriterierna bedömer vi också säkerheten och överensstämmelsen hos både de identifieringstjänster som erbjuds och nya tjänster. Även om kriterierna i första hand är avsedda för leverantörer av starka elektroniska identifieringstjänster och dem som bedömer dem, skapar de en god grund även för utvecklingen av andra identifieringstjänster.

I de uppdaterade kriterierna finns också en egen helhet för mobilidentifieringslösningar och -applikationer som används i identifieringstjänsterna. Dess mål är att förbättra säkerhetsnivån för de tillämpningar som nu används och som kommer att tas i bruk i framtiden. Kriterierna grundar sig på standarden för mobilapplikationer i The Open Web Application Security Project (OWASP), som vi anser skapar de bästa utgångspunkterna för utvecklingen av säkra applikationer. Kriterierna skulle inte ha färdigställts utan en utmärkt expertarbetsgrupp bestående av experter från tillverkare och leverantörer av identifieringstjänster.

Våra kriterier är unika globalt sett och har också väckt internationellt intresse. Flera tillsynsmyndigheter och aktörer som tillhandahåller identifieringslösningar och -tjänster har tacksamt tagit emot våra kriterier.

Mobilidentifieringslösningarna har blivit allt vanligare i snabb takt och det är klart att största delen av identifieringslösningarna i fortsättningen kommer att grunda sig på mobilterminalen och den identifieringsapplikation som installeras i den. Mobila lösningar har också synts i anmälningar som gjorts på basis av EU-medlemsländernas eIDAS-förordning och i yttranden från medlemsländernas samarbetsnätverk som föregår dessa. I utlåtandena har man särskilt tagit upp säkerhetsbedömningar i anslutning till förvaring av kryptografiska nycklar och lämpligheten hos biometriska verifieringsfaktorer. Du kan bekanta dig med vår anvisning 211/2019 O Anvisning om bedömning av elektroniska identifieringstjänster på vår webbplats. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/O211_Anvisning_om_bed%C3%B6mning_av_elektroniska_identifieringstj%C3%A4nster_211_2019_O_SV.pdf

Tillverkarna insåg fördelarna med Galileo

Den av EU-finansierade positioneringssatellittjänsten Galileo nådde 2019 en viktig etapp: En miljard terminaler som stöder användningen av öppen service i Galileo, främst smarttelefoner, hade sålts före september 2019. Årets största förändringstrend var att tillverkare började utnyttja Galileo.

Brexit gallrade bort systemets globala täckning

Galileo-systemet fungerade 2019 med sammanlagt 22 satelliter. Det ger global täckning. Storbritanniens avsikt att frigöra sig från EU ledde till att de brittiska delarna av Galileosystemets marksegment - säkerhetsövervakningscentrumet för Galileo i Storbritannien, och basstationerna på Falklandsöarna och Ascension - avskildes från helheten. För att jämna ut situationen inleddes byggandet av ett säkerhetsövervakningscentrum i Spanien.

Tjänsterna blir mångsidigare systematiskt fram till 2024

Galileos lokaliseringstjänster är tillsvidare i Initial Services-fasen. Det officiella ibruktagandet av en lokaliseringstjänst som är öppen för alla (OS, Open Service) torde ske i slutet av 2021. Övriga tjänster i Galileo tas i bruk en i taget och enligt en separat godkännandeprocess 2021–2024. Det största intresset kommer att riktas mot den kostnadsfria högprecisionstjänsten (HAS, High Accuracy Service) med 20 centimeters positionsnoggrannhet. Servicen anses vara viktig i synnerhet när autonoma trafikformer utvecklas.

Serviceavbrottet i juli väckte uppmärksamhet

I juli 2019 avbröts tjänsterna i nästan en vecka, med undantag av Search and Rescue, SAR-tjänsterna. Detta väckte förståelig uppmärksamhet inte bara i bland yrkesfolk utan också i den offentliga debatten. Användarna av tjänsterna upptäckte ingen stor förändring i sina satellitbaserade positioneringstjänster, eftersom konsumentterminalerna vanligen använder alla tillgängliga globala positioneringssatellitsystem, som förutom Galileo är GPS, GLONASS och BeiDou. Serviceavbrottet orsakades av ett mänskligt fel vid uppdatering av systemet. Händelsen har undersökts grundligt och för att undvika motsvarande fel har en rad åtgärder införts för att säkerställa verksamheten.

ÄVEN DU KAN HA GALILEO I DIN FICKA

EU:s satellitnavigationssystem Galileo producerar mycket exakta lokaliserings- och tidsuppgifter. Galileo drivs av Europeiska byrån för GNSS (GSA) under styrning av Europeiska kommissionen. Du kan också vara användare av Galileo, för en stor del av de nuvarande mobiltelefonerna och smarta apparaterna är riktade till konsumenter och utnyttjar redan Galileos satellit-signaler.

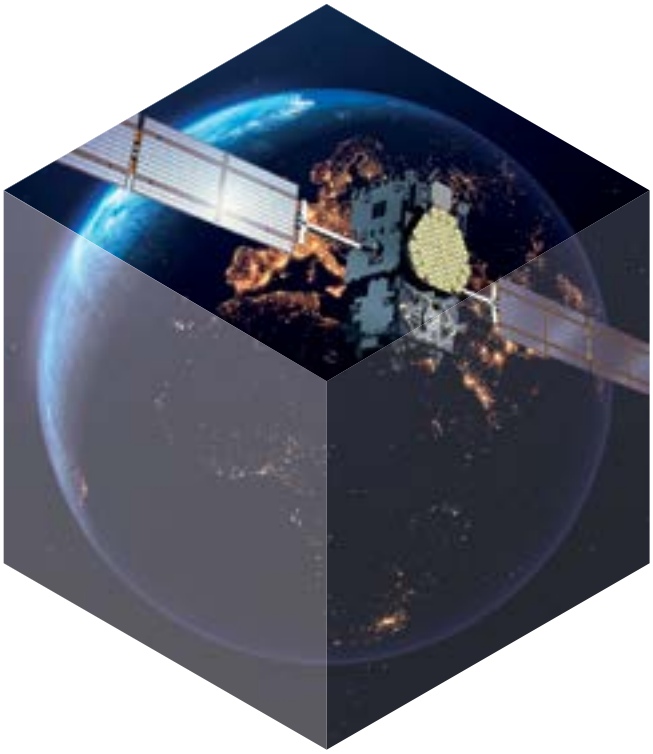
Kommunikationsministeriet överförde under 2019 ansvaret för beredningen av den operativa verksamheten inom de övriga Galileo-tjänsterna till vårt ämbetsverk. I månadsskiftet november–december 2019 ordnade vi en omfattande Galileo Innovation Challenge, som samlade en stor och internationell grupp deltagare i Helsingfors. Under evenemanget utvecklades nya sätt att använda tjänsterna i Galileo, undersöktes tekniker för att upptäcka störningar och innoverade sätt att kombinera Galileos tjänster med robotik. Evenemanget ingick i det åtgärdsprogram för satellitnavigering som ministeriet publicerade 2017.

Bättre precision och mindre störningar vid upptäckt av den amerikanska utrustningens Galileo-mottagningsförmåga

Efter att användningen av Galileo-frekvenser godkänts även i USA, började tillverkarna utnyttja Galileo under 2019. Galileos mottagningsförmåga som hittills varit dold i en del av de amerikanska terminalerna aktiverades via programuppdateringar. I smarttelefoner och andra avancerade mobilterminaler infördes processorer som innehöll möjligheten att ta emot signaler från Galileo - delvis även GPS - på två separata frekvensband, vilket har en positiv inverkan inte bara på positionsnoggrannheten utan också på signalens mottagning i stadsförhållanden. Den mest utbredda kretsen var Qualcomms Snapdragon 855.

Galileo-arbetet fortsätter och vi får mer ansvar

Som Finlands PRS- eller Galileo Public Regulated Service-myndighet fortsatte vi beredningen av ibruktagandet av PRS-tjänsten under ledning av kommunikationsministeriet. Flera områden inom statsförvaltningen och även företag som ansvarar för kritiska funktioner i samhället uttryckte sitt behov av att ta i bruk en verifierad lokaliserings- och tidstjänst. Avsikten är att den nationella PRS-användningen ska möjliggöra att planeringen av servicearkitekturen inleds 2020.



GALILEO INNOVATION CHALLENGE

Samarbete och informationsutbyte

Sammanställda nyheter från våra informationsutbytesgrupper

Våra informationsutbytesgrupper, ISAC (Information Sharing and Analysis Centre), är samarbetsorgan för cybersäkerhet som inrättats inom olika branscher. Deras huvudsakliga syfte är att sprida information och erfarenheter och därigenom öka organisationernas och branschernas förmåga att skydda sig mot digitala hot.

Vi använder den information som ISAC-grupperna producerar för att sammanställa en lägesbild över den nationella cybersäkerheten.

Här är de olika branschernas centrala nyheter från 2019.

BRANSCH	SÄRDRAG	AKTUELLT
STATSFÖRVALTNINGEN	Statsförvaltningens organisationer möter samma säkerhetshot som andra aktörer när det gäller förberedelserna inför valen och EU-ordförandeskapet. Iakttagandet av överenskommen praxis har räddat aktörer inom statsförvaltningen från många bedrägeriförsök, bland annat fakturerings- eller BEC-bedrägerier.	Beredskapen inför valet och EU-ordförandeskapet satte fart 2019. PiTuKri och Molnstrategin gav en gemensam syn på diskussionerna om molntjänster. I och med den nya cybersäkerhetsstrategin har ledningen av den nationella cybersäkerheten stärkts.
FINANS	Verksamheten inleddes våren 2019. Medlemmarna samarbetar för att utveckla branschen. Bluffmeddelanden som skickats i bankernas namn, samt överbelastningsangrepp mot aktörer är vardag.	EU:s rekommenderade TIBER-EU-ram styr branschen till regelbunden och scenariobaserad övning av hot. Praktiken ska grunda sig på så realistiska situationer som möjligt. TIBER-FI-ramen uppdateras och tillsammans med NIS-direktivet är de en del av rekommendations- och regleringsramen för aktörerna.
VATTENTJÄNSTER	Kärnan i affärsverksamheten är att automationssystemen fungerar, så skyddet och underhållet av dessa prioriteras.	Första året för gruppen ligger bakom. Man har delat erfarenheter, anvisningar, information och verktyg för att förbättra cybersäkerheten. Man planerar en fortsättning på projektet Cyber-Vatten från 2018. ISAC-gruppen deltar också i detta.
TELEFÖRETAG (ISP)	Teleföretagen och internetkontaktpunkterna har en speciell roll när det gäller att observera hot mot informationssäkerheten. Information om aktuella fall har spridits, diskuterats och använts i bekämpningen. Hotbilder som man diskuterar bekämpningen av är till exempel överbelastningsangrepp och illvilliga routningsändringar i internettrafiken.	Information om aktuella fall har delats, regleringens inverkan på affärsverksamheten och hur verksamhetssätten borde utvecklas för att man ska kunna svara på nya cybersäkerhetshot har diskuterats. Sommaren 2019 överfördes ordförandeskapet för informationsutbytesgruppen från Traficom till branschen.
SOCIAL- OCH HÄLSOVÅRD	Konfidentialitet och dataskydd i fråga om patient- och klientuppgifter är ständiga utmaningar som löses genom att sprida resultaten från projektet Cyber-Hälsa bland annat med hjälp av datasäkerhet. SHM publicerade den första nationella cybersäkerhetsanvisningen för social- och hälsovården. SHM skapar en riksomfattande verksamhetsmodell för branschen för att anmäla avvikelser i cybersäkerheten och skapa en lägesbild.	Spridningen av resultaten från projektet Cyber-Hälsa inleddes. Nya utvecklingsprojekt planeras. EU-lagstiftningen angående medicinsk utrustning ändras, och det kommer att medföra krav på cybersäkerheten. Informationshanteringslagen ändrade datasäkerhetskraven för social- och hälsovården.
ENERGI	Branschen har mycket gemensamt och egen övningsverksamhet. Det råder ett mycket starkt förtroende mellan aktörerna som gör det möjligt att aktivt dela information.	Aspekter på utnyttjande av IoT och molntjänster samt datasäkerhet. Diskussion om NIS-direktivet och bedömning av den tillhörande maturiteten hos cybersäkerheten. Inom branschen har man testat bedömningsverktyget Kybermittari som producerats av Cybersäkerhetscentret och Försörjningsberedskapscentralen. Med hjälp av verktyget kan företaget göra en självvärdering av sin maturitetsnivå inom cybersäkerheten.
KEMI OCH SKOGSINDUSTRI	Verksamhetens internationella karaktär samt ett starkt beroende av automationssystemen.	Bedrägerier kopplade till Office 365 har varit aktuella hela året. Särskilt talar man om beroendet av tjänsteleverantörerna och deras processer.
LIVSMEDEL OCH HANDEL OCH DISTRIBUTION	Livsmedelsproduktionen och handels- och distributionsbranschen är helt digitaliserade. Automation, robotik och IoT för att effektivisera affärsverksamheten är vardag.	Även inom denna bransch har i synnerhet O365-bedrägerierna varit till förtret för aktörerna. Dessutom sker införandet av ny teknologi i affärsprocesserna snabbt. Detta medför betydande utmaningar för den proaktiva hanteringen av datasäkerheten.
MEDIA	I branschen betonas nätförbindelsernas och systemens funktionssäkerhet både i nyhetsarbete med högt tempo och i den elektroniska kommunikationen. Dessutom är verksamheten och leverantörerna föremål för intresse, vilket bolagen också måste beakta när de sörjer för informationssäkerheten.	Mediebranschens beredskap inför cyberhot har stärkts såväl genom utbildning av personalen som genom datatekniska reformer, såsom användning av molnlösningar.
LOGISTIK OCH TRANSPORT	I och med den kraftiga digitaliseringen av transport- och logistikbranschen har man sett ett behov av att öka informationsutbytet om informationssäkerhet inom branschen.	L-ISAC inledde sin verksamhet i början av 2019 och nätverksarbetet har inletts väl.

Direktivet om nätverk och informationssystem NIS: EU:s medlemsstater rapporterade för första gången om informationssäkerhetsincidenter som var betydande för samhället

År 2019 var det första hela kalenderåret efter att direktivet om nätverk och informationssystem, mer känt som NIS-direktivet, trätt i kraft (5/2018). I februari 2020 rapporterade EU:s medlemsstater för första gången om hela årets (2019) betydande informationssäkerhetsincidenter. Den rapporterade informationen används för att utveckla cybersäkerheten både nationellt och inom EU.

NIS-direktivet ålägger leverantörer och aktörer som tillhandahåller kritisk infrastruktur i samhället minimiskyldigheter för riskhantering för nätverk och informationssystem, uppföljning och rapportering av informationssäkerhet. Skyldigheterna har införlivats i de nationella branschspecifika lagarna. I Finland övervakas dessa skyldigheter och de aktörer som är föremål för dem av sektorsvisa myndigheter. De rapporterar också avvikelser till oss på Cybersäkerhetscentret.

> ”För 2019 rapporterade Finland om en betydande informationssäkerhetsstörning inom hälso- och sjukvårdssektorn. Åtta andra betydande avvikelser rapporterades.

Under det gångna året rapporterade Finland om en betydande informationssäkerhetsstörning inom hälso- och sjukvården. Händelsen gällde en cyberattack och ett dataintrång mot kommunsektorn (läs mer på s. 36–37). År 2019 rapporterades åtta andra betydande avvikelser. Allt som allt var de väldigt lika händelserna 2018, som handlade om nätfiske med Office 365, hackade lösenord och olovliga inloggningar i system. Under direktivets första ofullständiga giltighetstid 2018 rapporterade Finland inga betydande avvikelser i informationssäkerheten.

Vi är Finlands kontaktpunkt i informationsutbytet mellan EU:s medlemsstater. Vi samordnar också det nationella och internationella samarbetet. Finlands sektorspecifika tillsynsmyndigheter har organiserat sig som NIS-samarbetsnätverk, som samlades fyra gånger 2019. En gemensam elektronisk blankett för anmälan om störningar är tillgänglig för aktörerna på vår webbplats. Myndighetsarbetsgruppen har också producerat presentationsmaterial och meddelanden åt aktörerna.

Blankett för anmälan om betydande störningar i nätverk och informationssystem för aktörer inom kritiska samhällssektorer:
https://www.kyberturvallisuuskeskus.fi/sv/vara-tjanster/rapportera-en-it-sakerhetsincident-nis-skyldighet

Energi
Energimyndigheten

- Innehavare av eldistributionsnät och högspänningsdistributionsnät
- Stamnätsinnehavare: Fingrid
- Innehavare av överföringsnät för naturgas: Gasum

Hälso- och sjukvård
Valvira

- Producenter av social- och hälsovårdstjänster
- Tillverkare av medicinsk utrustning
- Tillverkare av social- och hälsovårdens informationssystem

Finansbranschen
Finansinspektionen

- Banker
- Bankernas centralenheter
- EU-bankernas filialer

Finansbranschens infrastruktur
Finansinspektionen

- Börsen: Nasdaq

Trafik
Traficom

- **Luftfart:** Air Navigation Services Finland, Finavia Helsingfors–Vanda flygplats
- **Sjöfart:** Vessel Traffic Services Finland Oy; Åbo, Nådendal, HaminaKotka och Helsingfors hamnar
- **Järnvägstrafik:** Trafikledsverket som bannätsförvaltare, Finrail Oy
- **Landsvägstrafik:** Traffic Management Finland som trafikstyrningsbolag

Vattentjänster
Jord- och skogsbruksministeriet
NTM-centralerna

- Vattenverk: som levererar/tar emot över 5 000 m³ vatten/dygn

Digital infrastruktur
Traficom, Cybersäkerhetscentret

- Teleföretag (DNS)
- Universal transport points (IXP)
- DNS leverantörer av namntjänster
- .FI-landskodregister

Digitala tjänster
Traficom, Cybersäkerhetscentret

- Molntjänster
- Sökmotorer
- Nätets centraliserade marknadsplatser

Gäller inte små företag/mikroföretag

Skyldigheterna att rapportera om informationssäkerhet och störningar gäller aktörer inom energi-, trafik-, finans- och hälsovårdsbranschen samt vattenverk som levererar/tar emot över 5 000 m3 vatten/dygn. Även leverantörer av digitala tjänster, dvs. molntjänster, sökmotorer och stora och medelstora aktörer som tillhandahåller marknadsplatser på nätet omfattas av direktivets bestämmelser.

Rutinerat samarbete lade grunden för ett lugnt och smidigt EU-ordförandeskap

Beredskapen hålls uppe, även om man inte oroar sig för valresultatets tillförlitlighet

Det gångna året förde med sig två val - det nationella riksdagsvalet samt EU-valet. Val är en av demokratins grundpelare. Våra val är bland de säkraste i världen, om inte de säkraste.

Säkerhet är en känsla som vacklar inför olika hot och risker. Detta påverkas bland annat av förtroendet för myndigheternas förmåga att förebygga säkerhetshot. Till exempel är förtroendet för valprocessen nyckeln till detta. Vi ville vara med och trygga pålitliga val tillsammans med andra centrala myndigheter med anknytning till valet, så att störningarna i världen inte skulle få fotfäste i Finland.

I Sverige gjordes en överbelastningsangrepp mot systemet som hanterade valresultaten i valet 2018. I Frankrike hackade man partiets informationssystem och försökte skapa en skandal med hjälp av en dataläcka 2017, för att inte tala om presidentvalet i USA 2016.

Under riksdagsvalet i Finland utfördes en överbelastningsangrepp som Centralkriminalpolisen undersöker som misstänkt grovt störande av datatrafiken. I övrigt riktades valstörningarna mot enskilda kandidater.

Bakom våra nästan störningsfria val fanns ett nära myndighetssamarbete där vi fick delta. Tack vare samarbetet fick bland annat varje organisations roll i eventuella störningssituationer tydliga gränser. Alla visste vem de skulle kontakta om det skulle bli problem.

Finland som EU-ordförande

Valet förlöpte bekvämt, men redan efter ett par lugnare månader började en längre ansträngning. Finland var ordförandeland för EU från juli till december 2019. Under denna halvårsperiod ordnades flera minister- och tjänstemannamöten i Helsingfors, då Finland framhävdes som föremål för åtminstone de europeiska mediernas intresse. Man ville minimera den eventuella risken för sitt rykte. Säkerställandet av cyberdimensionen gjordes igen i gott samarbete med centrala myndigheter.

En sak ändras inte: det finns styrka i samarbete

Valet och EU-ordförandeskapet förlöpte på många sätt rutinmässigt ur ett samarbetsperspektiv. Nätverket för statsförvaltningen, som genomförs som ett ISAC-samarbete, erbjuder en utmärkt plattform för förtroende även i specialfall där Finland får mer uppmärksamhet.

Under 2018 skapade det intensifierade samarbetet inför mötet mellan president Trump och president Putin gemensam god praxis som också utnyttjades 2019. Även om samarbetsparterna kan växla något, hjälper samarbetet och förtroendet till att inleda varje beredskapsåtgärd. På så sätt kan man vid behov snabbt reagera även på överraskande störningar under normala förhållanden.

Genom valstörningar strävar man efter att rasera medborgarnas förtroende för samhället och det demokratiska system och det beslutsfattande som ligger till grund för det. Valstörningar kan också hänföra sig till mer omfattande målmedveten verksamhet eller hybridpåverkan.

Genom påverkan kan man bland annat försöka styra samhällsdebatten. På andra håll i världen har man observerat att valstörningar riktats mot röstningssystemet, väljare, partier och media.

CYBERSÄKERHETSCENTRET SÄKERSTÄLLER SÄKRA VAL

”Med tanke på datasäkerheten och informationssäkerheten var 2019 ett särskilt viktigt år för det finländska samhället. År 2019 ordnades två betydelsefulla val efter varandra i Finland. Under samma år tog Finland dessutom över ordförandeskapet för Europeiska unionen.

Vid evenemangen var det tydligt och mycket viktigt att garantera säkerheten i samarbete med olika myndigheter. Olika signaler från världen visade att man även i Finland borde förbereda sig på hot och att de blir verklighet. Redan före det första valet inledde myndigheterna ett nära samarbete för att valet skulle kunna hållas fritt i Finland, utan störningar. Ett nära samarbete garanterade också att myndigheterna kunde dela information mellan olika aktörer så snabbt som möjligt.

Ur Centralkriminalpolisens perspektiv kunde båda valen genomföras utan betydande störningar. Under riksdagsvalet utsattes resultattjänsten online för en kraftig överbelastningsangrepp, då resultattjänsternas webbplats tillfälligt upphörde att fungera. Gärningen kan redan i detta skede karakteriseras som en enskild handling och man kan inte se någon mer omfattande organiserad verksamhet mot just valet. Med hjälp av överbelastningsangrepp hade man inte möjlighet att påverka valresultatet. Det är dock ett allvarligt fenomen, eftersom attacken var riktad mot en viktig hörnsten i det fria demokratiska samhället.

Ur Centralkriminalpolisens perspektiv var beredskapen för att trygga valet tillräcklig och satsningen på detta mycket lönsam. Ur datasäkerhetssynpunkt kunde valet genomföras på ett mycket föredömligt sätt, vilket man särskilt kan tacka alla som var med och tryggade det för.

Med tanke på samarbetet mellan Centralkriminalpolisen och Cybersäkerhetscentret var 2019 mycket livligt. Vi satsade bland annat på varnande och förebyggande verksamhet i anslutning till intrång i Office 365. Med hjälp av omfattande informationsutbyte och informationskampanjer utökades finländarnas medvetenhet om fenomenet på ett betydande sätt. Vår satsning har även noterats ute i världen. Centralkriminalpolisen fortsätter att undersöka dataintrång, men i internationella kretsar åtnjuter Finland för närvarande särskilt gott rykte i anslutning till detta fenomen.

Marko Leponen
CKP

”I Finland är valen på många sätt beroende av datasystem och deras säkerhet, även om röstsedeln fylls i med penna och papper. Valdatasystemet som ägs av justitieministeriet och som innehåller bland annat rösträttsregistret och genom vilket valresultaten förmedlas, är centralt för att valet ska lyckas.

Arbetet mot valstörningar var intensivare än tidigare före riksdagsvalet och Europaparlamentsvalet våren 2019. Cybersäkerhetscentret tog en aktiv roll för att skapa av en lägesbild av valsäkerheten, förbättra myndighetssamarbetet och stödja upprätthållandet av valdatasystemet. Cybersäkerhetscentret sammanställde myndighetsnätverket Vaali-VIRT som bestod av alla intressentgrupper som var viktiga med tanke på valen. Nätverket övade tillsammans på hantering av störningssituationer, utbytte information och upprätthöll lägesbilden under valet med gemensamma lägesrapporter.

Ur justitieministeriets synvinkel var Cybersäkerhetscentralens insats för att trygga valet central. Faciliteringen av myndighetssamarbetet gav konkreta resultat. Cybersäkerhetscentrets experter identifierade de centrala aktörerna, hjälpte till att skapa en internationell lägesbild och stödde samarbetet.

Heini Huotarinen
JM

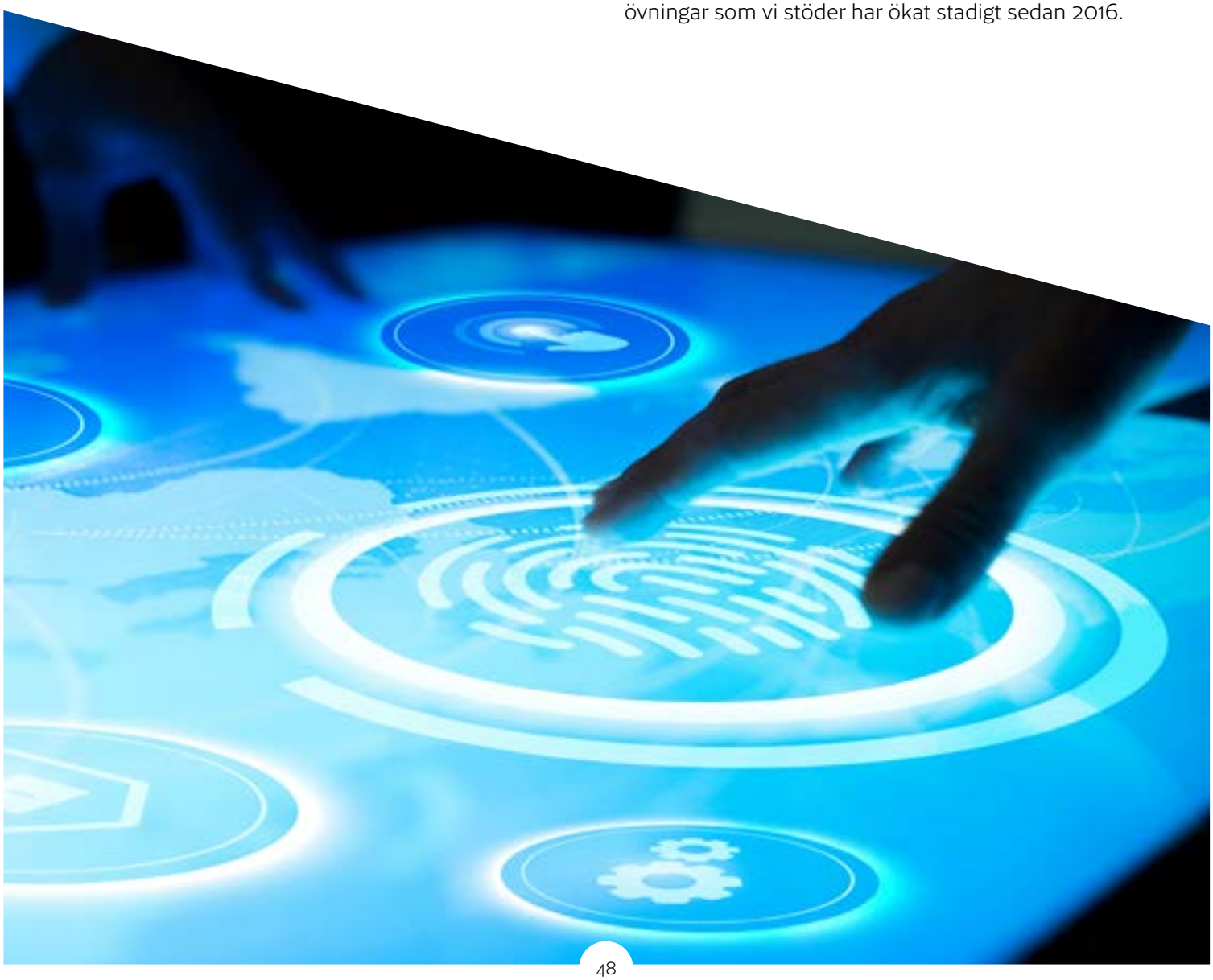
Cybersäkerheten behärskas bättre genom övning

Projekter blir en del av basservicen

Under 2019 har stödet för övningsverksamheten blivit en del av vår basservice. Planeringsarbetet som inleddes i samband med projektet KYBER 2020, som finansieras av Försörjningsberedskapscentralen, har gett en ny central del till vårt servicepaket. Övningsverksamhet tillsammans med andra tjänster hjälper oss att betjäna samhällets cybersäkerhet på ett allt mångsidigare sätt. Vårt stöd för övningsverksamheten fokuserar på att i huvudsak betjäna organisationer som är kritiska för försörjningsberedskapen genom handledning och stöd i frågor som rör övningsverksamheten.

Med hjälp av övning utvecklar organisationen handlingsberedskapen och reaktions- och återhämtningsförmågan och minskar därmed de skadliga effekterna av störningar och attacker. Deltagandet i övningarna har länge varit en del av vår verksamhet. Genom att delta i övningarna och simulera våra tjänster i dem har vi utvecklat vår egen verksamhet och hjälpt andra organisationer att öva realistiskt. Syftet med övningsverksamhetens stödfunktion är också att dela denna kompetens med andra kritiska aktörer.

År 2019 medförde rikligt med cyberövningar med hjälp av vilka företagen förbättrade sin egen beredskap och förmåga. Utgående från den respons vi fick upplevdes stödtjänsten för övningsverksamheten som nyttig och nödvändig även i fortsättningen. År 2019 visade att de försörjningsberedskapskritiska organisationernas vilja att förbättra sina egna cyberfärdigheter med hjälp av övningar har ökat. Antalet övningar som vi stöder har ökat stadigt sedan 2016.



Anvisningar för cyberövningar och övningsscenarier 2020

År 2019 publicerade vi en anvisning om cyberövningar där vi samlade lärdomar och erfarenheter från tiotals cyberövningar som samlats i vårt center, planeringen av dessa, spelandet samt analysen av resultaten. Med hjälp av anvisningen kan organisationen planera en cyberövning från början till slut antingen ensam eller tillsammans med en sakkunnig partner.

I slutet av 2019 ordnade vi också workshoppen Cyberövningsscenarier 2020. I den deltog representanter och myndigheter från centrala företag inom informationssäkerhetsbranschen. Som ett resultat av workshopen uppstod 20 övningsscenarier som stöd för organisationernas praktik. Scenarierna finns tillgängliga för alla på vår webbplats.

Vi fortsätter att utveckla övningsverksamheten

Vi fortsätter att kartlägga och identifiera träningsbehoven hos organisationer som är kritiska för försörjningsberedskapen även under de kommande åren. Med hjälp av en årlig enkät kartlägger man organisationernas önskemål och utmaningar samt följer upp förändringar i övningsförmågan och övningsviljan. Med hjälp av kartläggningen kommer vi även i fortsättningen att kontakta målorganisationerna och aktivt stöda organisationernas cyberövningar.

Utöver övningsstödåtgärderna som riktas till organisationer som är kritiska för försörjningsberedskapen sammanför stora gemensamma övningar, såsom TAISTO, ITO, KYHA och Cyber Europe flera försörjningsberedskapskritiska och andra organisationer.

Övningen FINEST19 förde samman Estlands och Finlands informationssäkerhetsmyndigheter

I mars övade vi tillsammans med den estniska datasäkerhetsmyndigheten CERT-EE på cyberstörning i den kritiska infrastrukturen i under övningen FINEST19. Övningen var den första internationella gemensamma övningen för Finlands och Estlands CERT-team som vi planerade och ordnade. Övningen genomfördes i samarbete med Finlands stamnätsbolag Fingrid och Estlands stamnätsbolag Elering.

Vi övade på en gemensam utredning av en cyberkris inom kritisk infrastruktur som drabbade båda länderna. Tyngdpunkten i övningen låg särskilt på effektiv och trygg kommunikation samt på att skapa en gemensam, delad lägesbild. Övningens scenario fokuserade på störningar i eldistributionen och det fanns också ett perspektiv som behandlade cyberbrottslighet.

Stöd för övningsverksamheten hjälper på följande sätt vid cyberövningar:

- planeringen av övningen inleds
- hitta en lämplig övningssamarbetspartner
- stöd för scenarioplanering
- simulering av cybersäkerhetscentralens tjänster under övningen
- observatörsroll i övningen
- assistans vid efteranalysen av övningen.

Framtidsarbete och utveckling av verksamheten

Cybersäkerhetsmärket kan erhållas av IoT-konsumentutrustning vars grundläggande informationssäkerhet är i skick

Cybersäkerhetsmärket hjälper konsumenterna att identifiera datasäkra apparater i butiken och webbshoppen och att göra datasäkra anskaffningar. Märket ökar också konsumenternas medvetenhet om hur smarta apparater används på ett säkert sätt. Med hjälp av cybersäkerhetsmärket uppmuntrar vi företagen att inkludera informationssäkerhetsegenskaper i sina apparater redan från början av produktplaneringen.

Vi beviljade det första cybersäkerhetsmärket till tre olika produkter: fitnessklockan Polar Ignite, Cozify Hub smarta hem och smarta termostaten DNA Wattinen. Våra pilotpartnerföretag Polar Electro Oy, Cozify Oy och DNA Abp har fäst särskild uppmärksamhet vid datasäkerheten i sina apparater redan innan de skaffade Cybersäkerhetsmärket. Denna förmåga i kombination med viljan att kommunicera datasäkerhetens betydelse för intressentgrupperna var centrala faktorer i valet av pilotpartner.

Cybersäkerhetsmärket visar riktningen för europeiska standarder för smarta apparater

För att en apparat eller tjänst ska kunna få Cybersäkerhetsmärket måste den uppfylla de krav som vi har fastställt. De baserar sig huvudsakligen på den europeiska standarden ETSI EN 303 645 Cyber Security for Consumer Internet of Things som fortfarande är i utkaststadiet. Vi deltar aktivt i utvecklingen av standarden för att säkerställa kompatibiliteten mellan eventuella allmäneuropeiska krav som kan träda i kraft senare. På detta sätt underlättas till exempel överföringen av finländska företag som tillverkar IoT-apparater till den internationella marknaden.

Certifieringen av IoT har väckt – och väcker fortfarande – stort intresse. Ämnet har också diskuterats i samband med certifieringssystemet för cybersäkerhet som EU inrättade i juni 2019. När ETSI:s standard färdigställs betraktas den som en möjlig grund för IoT-certifiering. Den myndighetsgrupp som bereder starten av certifieringssystemet har varit intresserad av vårt cybersäkerhetsmärke och man strävar efter att dra nytta av våra erfarenheter även i utvecklingen av den europeiska certifieringen.

Känt från tv, mer information på webbplatsen

Cybersäkerhetsmärket offentliggjordes den 26 november 2019. Vi gjorde märket känt genom kampanjer på tv och i sociala medier. När konsumenterna lär känna Cybersäkerhetsmärket och utbudet av apparater som fått märket växer, kan vi vara nöjda med märkets genomslagskraft. Mer information om bland annat kraven på Cybersäkerhetsmärket och hur du ansöker om det finns på adressen www.tietoturvamerkki.fi/sv/

Även om Cybersäkerhetsmärket är avsett för konsumentprodukter och -tjänster har även tillverkare som erbjuder företagslösningar varit intresserade av det. Kostnaderna för auditeringarna och den tid som använts för dem har väckt diskussion om huruvida man också borde göra en självvärderingsbaserad version av märket.

Vi kommer att granska utvecklingsmöjligheterna och slipa konceptet Cybersäkerhetsmärket utifrån våra erfarenheter. Vi kommer också att fortsätta att följa utvecklingen av de europeiska kraven. Om de eventuellt förändras har vi beredskap att också uppdatera våra egna krav. På så sätt kan vi bäst stöda finländska företags internationalisering.

Tietoturva


SOCIAL NETWORK
WEBSITE
MOBILE
SEO
MOBILE
WEBSITE

Användningen av utvidgningen av namntjänstens informationssäkerhet utvidgades avsevärt

Onödigt få med – avgiftsfri service har erbjudits sedan 2011

I Finlands FI-rotnamnstjänst DNSSEC togs i bruk stegvis i början av 2010-talet. Utöver FI-rotens DNSSEC-signatur erbjöd vi dem som använder fi-domännamn möjlighet att använda DNSSEC gratis.

Trots det tidiga ibruktagandet av tjänsten, avgiftsfriheten och många DNSSEC-kampanjer ökade inte användningen av DNSSEC nämnvärt i Finland.

I början av 2019 erbjöd domännamnsförmedlare av fi-domännamn i praktiken inte alls DNSSEC till sina kunder. Av fi-koderna var endast cirka 5 000 DNSSEC-skyddade. Cirka 7 procent av webbtrafiken i Finland gick via namnservrar som validerade DNSSEC.

Kampanj ökade användningen av DNSSEC glädjande mycket

I början av 2019 förde vi diskussioner med våra intressentgrupper och vi fick idén att ordna en nationell dag för ibruktagande av DNSSEC, DNSSEC Launch Day. Tanken var att samla de domännamnsförmedlare och internetaccesstjänster som förbinder sig att använda DNSSEC, upprätthålla en offentlig lista över dessa och ta upp behovet av DNSSEC i den offentliga debatten.

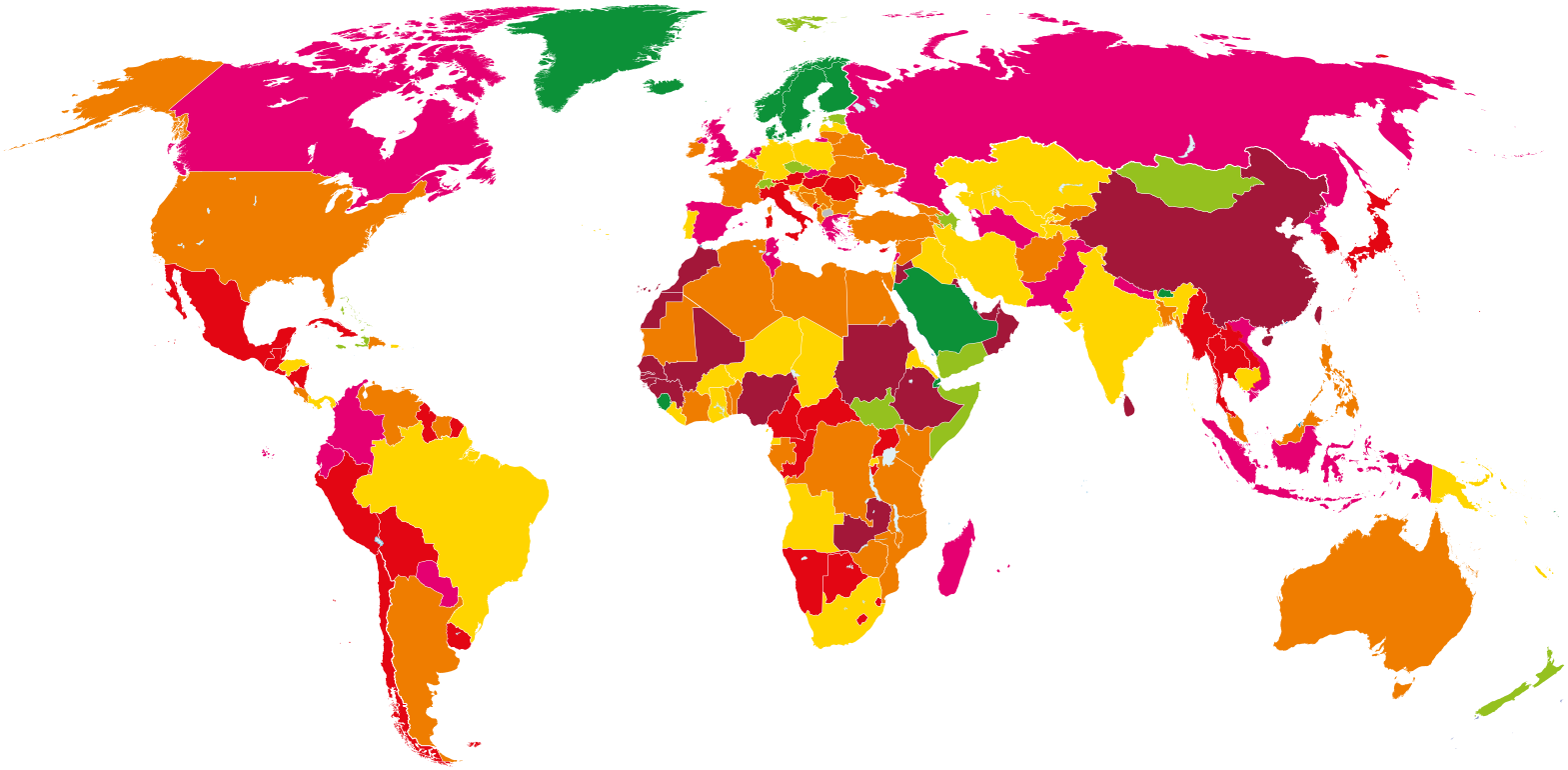
Ibruktagningsdagen fastställdes till den 5 september 2019. I kampanjen deltog 33 domännamnsförmedlare och 3 internetleverantörer.

Antalet domännamnsförmedlare som erbjuder DNSSEC ökade betydligt. I slutet av 2019 erbjöd redan över 250 fi-domännamnsförmedlare sina kunder DNSSEC och nästan 10 000 fi-domännamn hade DNSSEC-signatur. Siffran är dubbelt så stor som 2018.

DNSSEC-valideringsgraden steg under året från 7 procent till över 90 procent när stora inhemska internetanslutningsleverantörer tog i bruk valideringen i sina resolvernamnsservrar. Även globalt sett är den valideringsgrad som uppnåtts hög.

Domain Name Security Extensions (DNSSEC) är en teknik som säkerställer äktheten och oföränderligheten i namntjänstens svar. Med hjälp av DNSSEC är det möjligt att verifiera namntjänstens svar eller en förfalskning av resolvernamnsserverns cacheminne. DNSSEC är en av de viktigaste informationssäkerhetsegenskaperna med hjälp av vilka man säkerställer att till exempel adressen och innehållet på den webbplats som användaren har öppnat motsvarar varandra och att e-posten hamnar hos mottagaren enligt adressen.
Det är dock inte tillräckligt att skydda domännamnet med DNSSEC för att det ska gynna internetanvändare. DNSSEC-signaturen måste också verifieras i internettrafiken, annars kommer även DNS svar där DNSSEC-signaturen är felaktig att hamna hos internetanvändare. För verifieringen eller valideringen ansvarar resolvernamnsservrarna, som vanligen upprätthålls av dem som tillhandahåller internetanslutningar.

DNSSEC Validation Rate by country (%)



SIFFROR

265 Antal fi-domännamnsförmedlare som erbjuder DNSSEC till sina kunder (st.):

10 255 Antal DNSSEC-skyddade fi-domännamn (st.)

92,2% DNSSEC-valideringsgrad i Finland:

Arbetet med att trygga informationssäkerheten i 5G-näten fortsätter

Arbetet som inleddes 2018 med en cybersäkerhetsutredning av 5G-näten fick en fortsättning. År 2019 följdes utredningen av en riskbedömning av 5G på nationell nivå och EU-nivå.

Nu arbetar EU för att utveckla en verktygslåda som stöder riskhantering av 5G-näten. Arbetet resulterar i information som gör det möjligt för aktörer som tillhandahåller och använder 5G-teknologi att göra realistiska riskbedömningar och skapa säkra lösningar.

Som en del av arbetet har man identifierat att övergången till 5G-teknologi medför ett större paradigmskifte än någon tidigare generation av mobilnät har gjort. Ibruktagande av 5G-teknologins nya egenskaper och verksamhetsmodeller förändrar operatörernas roll, medför skräddarsydda nätverk för lokala behov, kan utvidga myndighetsstyrningens verksamhetsfält och införa helt nya riskhanteringskrav för aktörer som utnyttjar 5G-egenskaper. Nätet går från att vara ett rör för dataöverföring till en allt mer delad plattform för att producera och hantera data där nätverkets gränser suddas ut. Detta skapar utrymme för nya funktioner och möjligheter som även aktörer som tillhandahåller samhällskritiska funktioner kommer att använda. Samtidigt kommer samhällets allt viktigare funktioner att förlita sig på 5G-näten.

Förändringen från den tidigare nätgenerationen till en 5G-värld kommer att kräva aktiv delning av information, omprövning av gränserna för myndighetsstyrningen och en allt mer omfattande dialog mellan olika aktörer samt slutligen även nya myndighetsorder. På internationell nivå kommer även nationella och EU-omfattande rekommendationer, lagar och författningar att innebära en utmaning för informationssäkerheten i 5G.

Utöver den teoretiska approachen ville vi som samarbete på EU-nivå främja även det tekniska kunnandet i informationssäkerhetssystemet som bygger på 5G-tekniken. För att föra hackar- och datasäkerhetstestgemenskapen, tillverkarna av utrustning, Cybersäkerhetscentret och vetenskapsvärlden närmare varandra, ordnade vi 29.11–1.12.2019 i samarbete med Uleåborgs universitet, Ericsson och Nokia 5G Cyber Security Hackathon, det första hackathon-evenemanget i världen som fokuserar på 5G:s informationssäkerhet.

I det deltog nästan 100 hackers från över 10 olika länder och det gav alla parter ett unikt tillfälle att lära sig nya saker. Analysen av resultaten pågår och lärdomarna från hackathon kommer att delas och erfarenheterna diskuteras med beslutsfattarna i den digitala världen den 13 februari 2020 i 5G Leading Edge Forum.

Kyber 2020 och Digital säkerhet 2030

Vi har ett aktivt utvecklingsår för vår verksamhet bakom oss. Till exempel förbättrade vi nätverksledningen (ISAC-verksamheten) och övningsverksamheten i enlighet med Försörjningsberedskapscentralens program KYBER 2020. Vi gjorde också avgörande framsteg i utvecklingen av HAVARO-tjänsten. Utifrån kundresponsen har vi upplevt att vårt utvecklingsarbete är nödvändigt.

Mer stöd till företag som är kritiska för försörjningsberedskapen

Just för företag som är kritiska för försörjningsberedskapen har utvecklingen av vår verksamhet visat sig som nya tjänster och skicklighet samt ett ännu mer fungerande samarbete. Tillsammans med Försörjningsberedskapscentralen har vi byggt upp förtroendet bland annat genom att delta i utvecklingen av den sektor- och poolspecifika cybersäkerheten.

En stark nationell cybersäkerhet byggs upp

Försörjningsberedskapscentralens program KYBER 2020 får en fortsättning med programmet Digital säkerhet 2030, vars planeringsarbete inleddes 2019.

Syftet med programmet Digital säkerhet 2030 är att utveckla den nationella cybersäkerheten djupare och med en större grupp än tidigare. Vi har deltagit aktivt i planeringen av programmet, dit även näringslivet och poolverksamheten har bjudits in.

År 2019 fick programmet ett strategiskt mål, centrala innehåll och verksamhetssätt med hjälp av vilka målen uppnås. Programmet förs vidare enligt en smidig utvecklingsmodell och man vill engagera såväl näringslivet som myndigheterna i programmet.

Det nya samarbetsavtalet ger långtgående möjligheter

Under det gångna året ingick vi ett nytt samarbetsavtal med Försörjningsberedskapscentralen som garanterar att vår verksamhet får minst 4 000 000 euro i årlig finansiering. Det kommer att göra det möjligt för oss att arbeta systematiskt för kontinuitet och säkerhet i företag som är kritiska för försörjningsberedskapen.

Som en del av programmet har vi utarbetat vår egen utvecklingsplan. I fortsättningen kan vi till exempel bättre än tidigare beakta de strategiska målen för utvecklingen av Försörjningsberedskapscentralens cybersäkerhet. Dessutom har vi velat förbättra vår funktionsförmåga så att den kan skalas upp bättre än tidigare i omfattande störningssituationer. Nya tjänster som vi kan använda för att få bättre lägesdata och identifiera nya hot har också inkluderats i planen.

Försörjningsberedskapscentralen är en pålitlig samarbetspartner som också stöder vår verksamhet och dess utveckling.

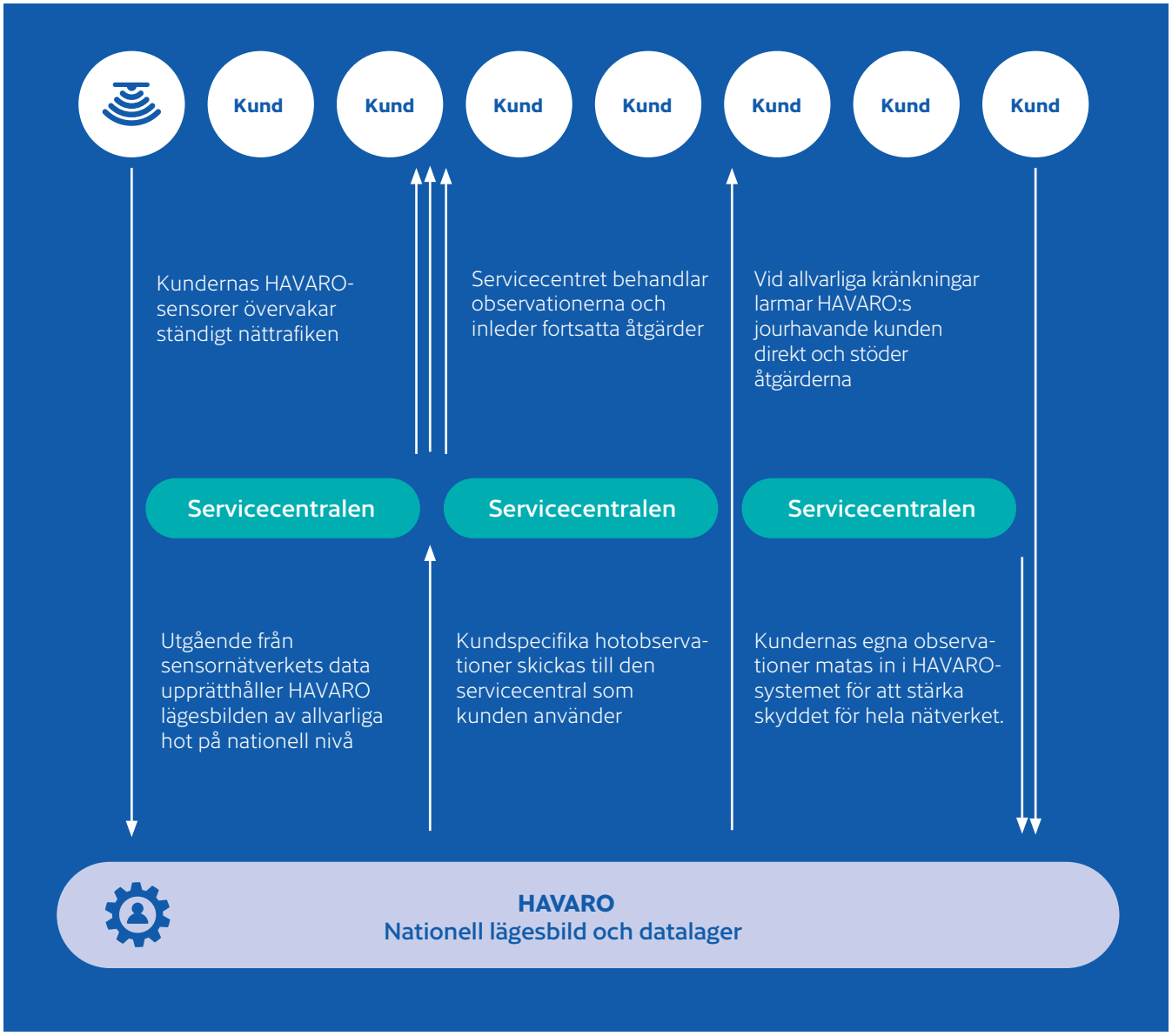
Välkommen som kund i den förnyade HAVARO-tjänsten!

Vår HAVARO-tjänst varnar kunderna för skadlig trafik och gör det möjligt att avvärja hot mot informationssäkerheten. Kunderna är nu företag som är kritiska för försörjningsberedskapen och statsförvaltningens organisationer. Genom att utnyttja skadlig trafik kan en utomstående aktör till exempel komma åt kundens affärshemligheter eller orsaka ekonomiska förluster genom att påverka kundens transaktioner.

Förnyelsen av HAVARO-tjänsten inleddes 2017 som en del av Försörjningsberedskapscentralens projekt KYBER 2020. Den nya tjänsten framskrider till produktionsfasen under 2020.

Det blir lättare att skaffa tjänsten

HAVARO blir tillgängligt för finländska organisationer sommaren 2020 då tjänsten blir en del av utbudet hos kommersiella servicecentraler (SOC) som tillhandahåller informationssäkerhetstjänster.



HAVARO-tjänstens servicemodell

Den nya servicemodellen ersätter den myndighetsversion av HAVARO som vi har producerat sedan 2011. HAVARO, som bygger på samarbete mellan Cybersäkerhetscentret och kommersiella informationssäkerhetsaktörer, kommer att svara mer övergripande och noggrannare än tidigare på kundernas behov.

Framtidens behov

I planeringen och genomförandet av den nya tjänsten har vi också beaktat framtidens utvecklingsbehov och krav. Under projektets gång har vi fört många konstruktiva diskussioner med både våra kunder och andra intressentgrupper. Vi har fått värdefull respons och utvecklingsidéer under många workshoppar och gemensamma evenemang.

Vår samarbetspartner i utvecklingen av tjänsten är Reaktor Innovations Oy. Genom tillämpning av agil systemutveckling har det nya systemet och dess komponenter testats i god tid och stegvis fåtts i produktion.

Det finns plats för nya samarbetspartner

Under 2019 preciserades HAVARO:s nya service- och verksamhetsmodell i samarbete med servicecentren. Vi förtydligade villkoren för tjänsten som gör det möjligt att erbjuda HAVARO-tjänsten på ett högklassigt sätt, men på ett sätt som motsvarar olika kundbehov.

Även nya samarbetspartner är välkomna till det ekosystem som HAVARO-tjänsten bildar. Vi tar gärna emot till exempel servicecentralsaktörer och teknologileverantörer. Välkommen med att bygga en finländsk grundpelare för cybersäkerhet!

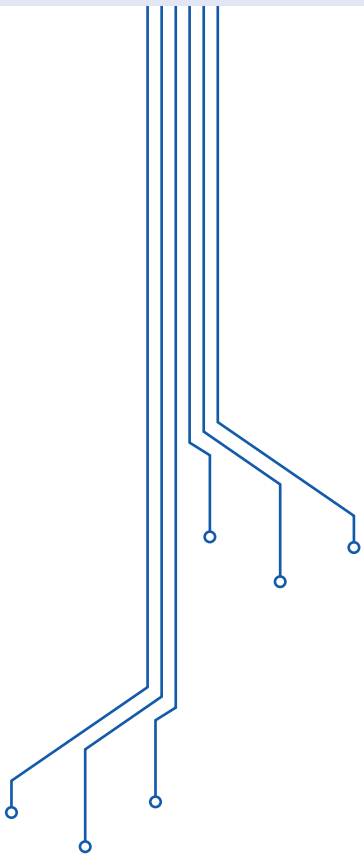
Sårbarhetskoordinering

Det viktigaste fallet i årets sårbarhetskoordinering var sårbarheten hos byggnadsautomationsapparater av märket Fidelix.

I mars 2019 testade en grupp hackare byggnadsautomationsapparater av märket Fidelix i Yles programserie Team Whack och hittade flera sårbarheter i dem. Vi koordinerar korrigeringen av dessa sårbarheter och informationen apparaternas ägare. Trots vårt informationsarbete minskade antalet öppna och oskyddade apparater på internet långsamt med undantag av utrustning som administreras av tredje part.

De öppna byggnadsautomationsapparaterna som syns på internet har funnits i våra informationssäkerhetskartläggningar av de inhemska datanäten redan i flera år. Byggnadsautomationsapparaternas svagheter kunde utnyttjas av angripare för att skada dem som använder byggnaderna. Det har dock varit svårt att nå anläggningarnas ägare och därför har antalet öppna apparater inte minskat nämnvärt.

Vår sårbarhetssamordning hjälper den som upptäcker en sårbarhet eller ett allvarligt programfel att samarbeta till exempel med programvarutillverkaren. Vi behandlar alltid sårbarhetsuppgifter ansvarsfullt. Vårt mål är att informationen om sårbarheten och en ändamålsenlig korrigering av den jämte uppdateringar ska nå alla som behöver informationen, även produktens slutanvändare. Vi strävar efter att även reparera så många betydande sårbarheter som möjligt och att införa reparationerna.



Nyckeltal för vår verksamhet

Enligt siffrorna var 2019 arbetsfyllt för oss. Nedtagning av skadliga sidor och informationsutbytesgruppernas evenemang höll oss sysselsatta, men i övrigt följde det gångna året samma takt som i fjol.

24/7/365
Oavbruten jour

2
Varningar

83208
Auto-reporter

4500
Behandlade fall

25
Fall som hanterats av sårbarhetskoordineringen

4500
Nedtagning av skadliga webbplatser

5500
Facebook-följare

11000
Twitter-följare

Antal störningar

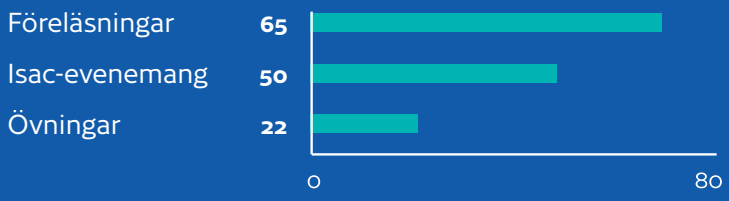
7
Kritiska störningar

18
Allvarliga störningar

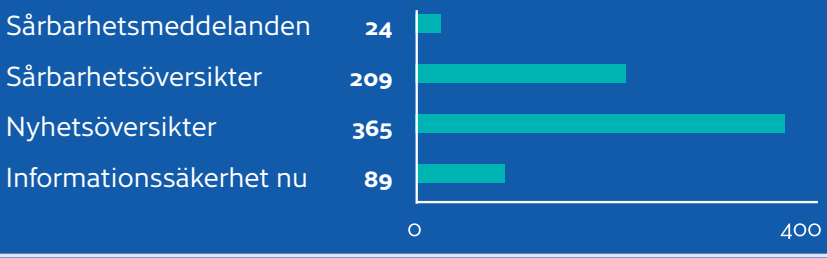
43
Betydande störningar

68
Alla störningar totalt

Möten och övningar



Kommunikation och meddelanden



Under året genomförde vi kundnöjdhetsenkäter om våra lägesbildsprodukter och informationsutbytesgrupper. Bedömningsskalan för våra enkäter var från dålig (1) till berömlig (5).

De branschspecifika informationsutbytesgrupperna bedömdes vara till nytta. Särskilt viktig ansågs möjligheten till informationsutbyte och nätverkande.

Man är nöjda med våra lägesbildsprodukter

4,2
Genomsnitt

Enkät till branschernas informationsutbytesgrupper

4,4
Vitsord

CYBERVÄDRET 2019 OCH EN BLICK MOT 2020

”Man känner inte tillräckligt till cyberbrottslighetens karaktär. Största delen av cyberbrottsligheten är opportunistisk, internationell och automatiserad. När en person eller organisation bedömer sin egen risk för att bli föremål för informationssäkerhetsincidenter, antar man att man måste vara ett objekt som intresserar angriparen, även om man vanligtvis blir objekt slumpmässigt.

Tio utsikter för informationssäkerheten 2020

Utsikterna för informationssäkerheten 2020 grundar sig på en gemensam bedömning av Cybersäkerhetscentret och våra samarbetsnätverk. Fick vi rätt i våra utsikter, syns det i slutet av 2020.

1 Automatiserade informationssäkerhetslösningar som använder artificiell intelligens växer fram

I takt med att utbudet ökar, ökar även bland annat SOC-tjänsternas användning och blir mångsidigare.

2 Tjänster kommer att produceras i multinationella entreprenörskedjor med många skikt

I utlokaliseringsskedet är det väsentligt att utreda och precisera de komponenter, beroendeförhållanden och ansvar som är väsentliga med tanke på datasäkerheten. I efterhand är förändringarna ofta utmanande, särskilt om bristerna framkommer först vid avvikelser. Samma problem gäller såväl privata som offentliga organisationer. Störningar i tjänsterna kan också störa samhällets funktion.

3 Cybersäkerhetens inverkan på affärsverksamheten beaktas bättre än tidigare

Affärsverksamheten är beroende av digitalisering. De risker som är förknippade med detta måste integreras rutinmässigt i riskhanteringsåtgärderna. Man har vaknat upp till situationen, vilket syns som ett behov av riskbaserade granskningsmodeller i anslutning till datasäkerhetsverksamheten.

4 Skyddet haltar eftersom cyberbrottslighetens natur inte är tillräckligt känd

Största delen av cyberbrottsligheten är opportunistisk, internationell och automatiserad. När en person eller organisation bedömer sin egen risk att råka ut för en informationssäkerhetsincident, antar man att man måste vara ett objekt som intresserar angriparen, även om man vanligtvis blir objekt slumpmässigt.

5 Allt fler ordnar cybersäkerhetsövningar

Verksamheten är ofta välplanerad, men i verkligheten kan nödsituationer och kaos överraska. För att åtgärda situationen övar allt fler organisationer på att agera i störningssituationer och utvecklar sin verksamhet bland annat utifrån observerade brister.

6 Informationssäkerhetshål som hittas utnyttjas allt snabbare

Rutinmässiga processer för publicering och uppdatering av uppdateringar räcker inte längre till. Som stöd för programuppdateringar måste man ta fram nya skyddslösningar som kan förbättra observationerna.

7 Behovet av mångkunniga experter på informationssäkerhet ökar

De tekniska experternas kompetens inom datasäkerhet håller på att differentieras till olika delområden. Bland experterna behövs också personer som har förståelse för affärsverksamhet och bland annat icke-teknisk kompetens i anslutning till upphandling.

8 Information och verksamhet flyttar till molnet

Molntjänsterna blir mångsidigare. I stället för enbart lagringsutrymme erbjuder molntjänster centraliserade funktioner som traditionellt har genomförts i det egna nätverket. Frågan om följande tjänster blir allt viktigare: Är ansvarsfördelningen mellan molnleverantören och organisationen klar?

9 Informationssäkerhetsbedömningar blir vanligare vartefter medvetenheten ökar

Säkerställandet av informationssäkerhetskompetensen och -nivån blir allt viktigare. Det blir lättare att påvisa detta till exempel för kunderna när bedömningen genomförs av en utomstående aktör.

10 Det finns ett samband mellan informationssäkerhetsnivån och personalens medvetenhet

I organisationerna framkommer informationssäkerhetens styrkor och svagheter via personalen. Även en enskild anställd kan avvisa e-post som innehåller till exempel nätfiske, faktureringsbedrägerier eller skadliga program. Det lönar sig att satsa på utbildningar och övningar!

Hur lyckades vi bedöma datasäkerhetsutsikterna för det gångna året?

Våra bedömningar var bra! Alla våra utsikter höll streck.

Rätt!

Vi hade förberett oss på en ökad användning av molntjänster och på att nya teknologier och utmaningar i anslutning till dem skulle dyka upp. I takt med att utbudet ökade såg vi också att trenden med att lägga ut informationssäkerheten på entreprenad fortsatte.

Sakta men säkert upptäckte vi att datasäkerheten blev organisationernas övergripande riskhantering och förbättrade skyddet mot cyberhot. Det behövs verkligen skyddsåtgärder i takt med att nätbrottslighet blir vanligare och cyberattacker mot statliga aktörernas blir vanligare.

På sommaren talades det om störningarna i kommuntjänsterna. Fallen visade på ett tråkigt sätt hur beroende av digitala tjänster skapar överraskande men också allvarliga situationer.

Behovet av grundläggande kunskaper i informationssäkerhet och den mänskliga sidan lyftes fram. Ämnet är också aktuellt nu. Till exempel personalens datasäkerhetsfärdigheter och förmåga att identifiera nätbedrägerier förbättrar väsentligt hela samhällets säkerhet. Även i Finland var läckage av användarnamn och betalningsbedrägerier som verkar oskyldiga vardagsmat.

Även om säkerheten hos apparater som ansluts till internet inte har förbättrats under det senaste decenniet, syns även ljusglimtar, eftersom identifieringen av säkra konsumentprodukter underlättades med hjälp av Cybersäkerhetsmärket.

1	**Molnet är på stadig frammarsch och förändringen gläder och oroar**	Jaa
2	**Allt fler utkontrakterar informationssäkerhet**	Jaa
3	**Statliga aktörers cyberangrepp och nyhetsrapporteringen om dem fortsätter**	Jaa
4	**Det finns fortfarande en del att förbättra i organisationers grundläggande informationssäkerhet**	Jaa
5	**Informationssäkerhet blir en del av riskhantering som utgår från affärsverksamheten**	Jaa
6	**Den mänskliga aspekten av i nformationssäkerhet blir större**	Jaa
8	**Informationssäkerheten hos konsumentprodukter som ansluts till internet blir allt viktigare**	Jaa
7	**Beroendet av digitala tjänster skapar överraskande situationer**	Jaa
9	**Kända hot som klassats som blir sakta värre**	Jaa
10	**Den nya tekniken bestämmer hur utmaningarna för informationssäkerheten ser ut på 2020-talet**	Jaa
+1	**Ingen epidemi av skadeprogram riktade mot mobila enheter kommer at ses**	Jaa

Cybervädret 2019

Januari

Stormen Aapeli gick särskilt hårt åt kommunikationsnäten på Åland

Skadlig verksamhet spreds via den öppna RDP-fjärrhanteringen på internet

Februari

Antalet vd-bedrägerier har ökat. Vid bedrägerier utnyttjas hackade e-postkonton i Office 365

Cyberbrottslingarna tjänade miljoner på vd-bedrägerier och big game hunting

Mars

Blockeringsattacker i flera europeiska länder i syfte att störa val

Dataintrång i Norsk Hydro orsakade stora ekonomiska förluster

Många IoT-apparater i Finland ligger öppet på internet. Ämnet behandlades i Yles program Team Whack.

April

I webbtjänsten för resultaten från riksdagsvalens gjordes en överbelastningsangrepp

Amerikanska NSA:s spionverktyg misstänks ha kommit i händerna på en kinesisk grupp

Maj

Bluekeep-sårbarheten kan leda till en epidemi med skadliga program som sprider sig självständigt

Big game hunting-grupperna utnyttjar allmänna skadliga program

Juni

Varning 01/2019: E-postservern Exims sårbarhet utnyttjas för dataintrång

Kommunfall: Lahtis

Rikligt med porrutpressnin bedrägerier anmäldes

Ga ur

Ko

= Internationella nyheter

Juli

ileostörning, tjänsten
oruk en vecka

mmunfall: Kumo

Augusti

Statsförvaltningens webbplats föremål för överbelastningsangrepp

Varning 02/2019: Microsofts distansarbetsbord har sårbarheter som utnyttjas vid dataintrång

Kommunfall: Björneborg

September

Vi tog bort en varning om intrång i Office 365

Cyberbrottslingar greps i internationella operationer

Oktober

På 15 år har IoT-apparaternas datasäkerhet inte förbättrats

Allmänt spritt fynd i nätverksdiskar som gäller skadliga programmet QSnatch

De som spionerar efter uppfinningar samlar också in information om personer.

Speglande överbelastningsangrepp

November

Cybersäkerhetsmärket hjälper konsumenter att göra säkrare anskaffningar av smarta apparater i hemmet – Finland inleder som första land i Europa tryggande av smarta apparater

En identifiering i flera skeden skulle förebygga största delen av datainträngen i Office 365

December

Vår årliga kartläggning avslöjade än en gång över 1 000 oskyddade apparater i inhemska datanät

Abonnemangsfällor spreds via textmeddelande, e-post och reklamlänkar samt med hjälp av sökmotoroptimering

Ibruktagandet av DNSSEC-datasäkerhetsutvidgningen fick en bra start

Livligt år för publikationer, evenemang och kampanjer

Här är några exempel från vårt livliga publikationsår 2019.
Förhoppningsvis fick så många som möjligt hjälp av våra guider och kampanjer.

KAMPANJER OCH EVENEMANG

Säkerhetsisten Teijo delade poänger igen
https://turvalistit.fi/se

Cybersäkerhetsmärket hjälper till att göra smarta köp av smarta apparater
https://tietoturvamerkki.fi/sv/

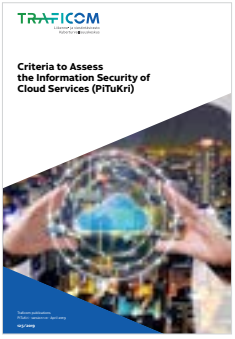
Världens första 5G-cybersäkerhetshackathon
https://www.kyberturvallisuuskeskus.fi/sv/aktuellt/70-topphackare-fran-alla-delar-av-varlden-samlades-i-finland-varldens-forsta-oppna-5g

GALILEO INNOVATION CHALLENGE

Galileo Innovation Challenge: Internationella lag utvecklar tjänster för EU:s Galileo-satellitpositionering
https://www.kyberturvallisuuskeskus.fi/sv/aktuellt/internationella-team-i-helsingfors-skapar-nya-tjanster-eus-satellitnavigationssystem

PUBLIKATIONER

Skydd mot fiske och dataintrång i Microsoft Office 365.
Även engelsk översättning finns tillgänglig.
https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Office365_SE_WEB_160420.pdf



Säkerhetskriterier för molntjänster (på finska)
https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri_v1_1.pdf

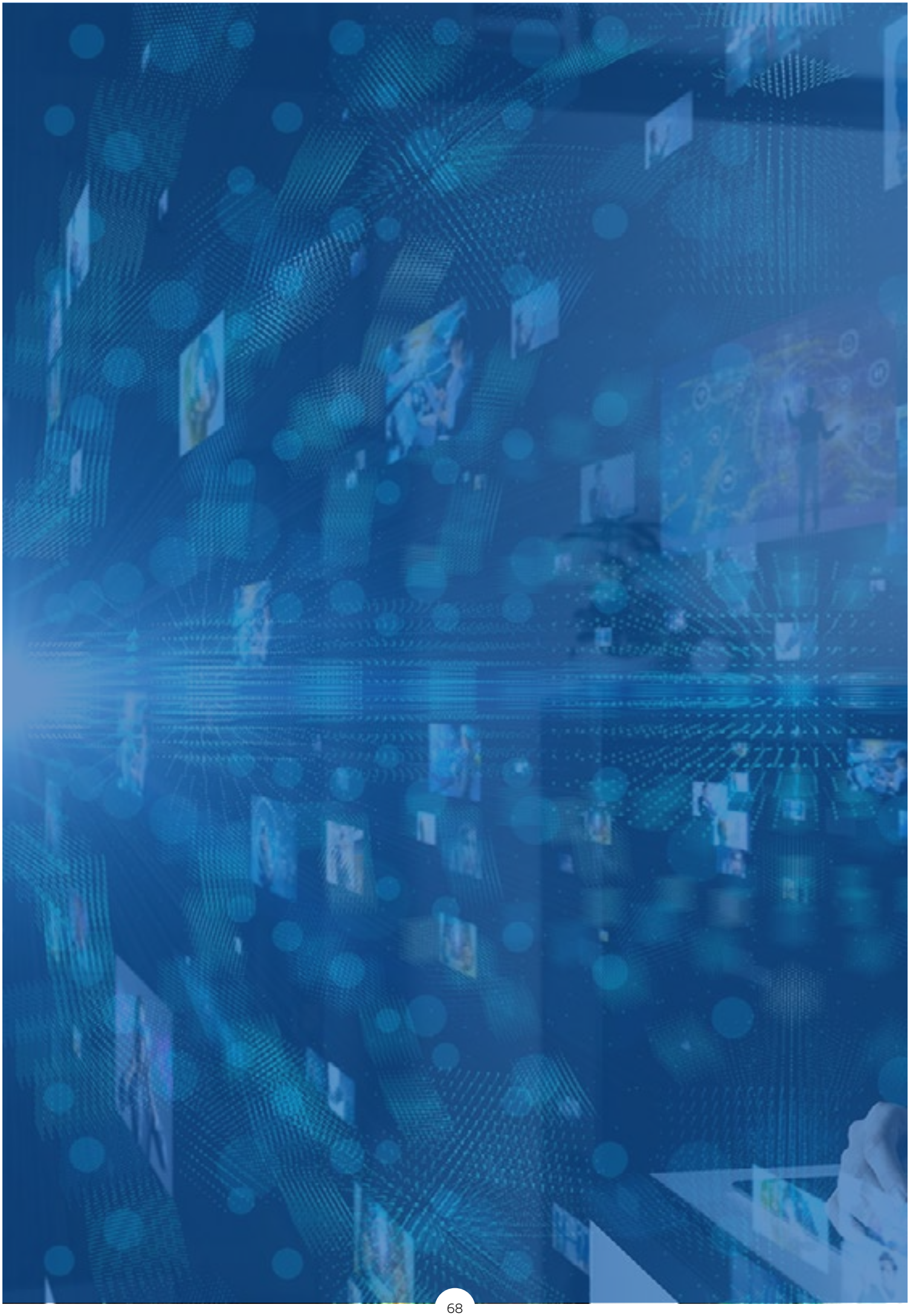
Säkerhetskriterier för molntjänster, engelskspråkig översättning
https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/PiTuKri_v1_0_english.pdf

Anvisning för cyberövning – Handbok för arrangören av övningen (på finska)
https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kyberharjoitusopas.pdf

Guiderna Tryggt på webben för barn och föräldrar (på finska)
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/turvallisesti-netissa-oppaat-lapsille

BEKANTA DIG ÄVEN MED FÖLJANDE

- Källan till förtroende – Perspektiv på standardisering och certifiering av informationssäkerhet (på finska) https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Luottamuksen_lahteilla.pdf
- Så här skyddar du dig mot nätbedrägerier https://www.kyberturvallisuuskeskus.fi/sv/aktuellt/anvisningar-och-guider/sa-skyddar-du-dig-mot-natbedragerier
- Så här sörjer du för informationssäkerheten hemma och på arbetsplatsen https://www.kyberturvallisuuskeskus.fi/sv/aktuellt/anvisningar-och-guider/sa-har-sorjer-du-informationssakerheten-hemma-och-pa-arbetsplatsen
- Projektet Cyber-Hälsa: Krav på informationssäkerhet och dataskydd vid upphandling inom social- och hälsovården (på finska) https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/sosiaali-ja-terveydenhuollon-hankintojen-tietoturva-ja
- Bedömningsanvisning för elektronisk identifieringstjänst https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/O211_Anvisning_om_bed%C3%B6mning_av_elektroniska_identifieringstj%C3%A4nster_211_2019_O_SV.pdf



Nyhetssammanställning om cybervädret 2019

Januari

- Stormen Aapeli gick särskilt hårt åt kommunikationsnäten på Åland (på finska) https://yle.fi/uutiset/3-10578072

Februari

- Antalet vd-bedrägerier har ökat. Vid bedrägerier utnyttjas hackade e-postkonton i Office 365 (på finska) https://yle.fi/uutiset/3-10676320
- Cyberbrottslingarna tjänade miljoner på vd-bedrägerier och big game hunting (i engelska) https://www.crowdstrike.com/blog/pinchy-spider-adopts-big-game-hunting/

Mars

- Dataintrång i Norsk Hydro orsakade stora ekonomiska förluster (på finska) https://www.tivi.fi/uutiset/kiristyshaittaohjelma-aiheutti-pohjoismaiselle-yhtiolle-viikossa-jopa-36-miljoonan-euron-tappiot/abfb80fb-6078-3c89-8869-9567673ea39d
- Många IoT-apparater i Finland ligger öppet på internet. https://www.kyberturvallisuuskeskus.fi/sv/aktuellt/vem-slackte-ljuset-bristfallig-informationssakerhet-av-uppkopplad

April

- I webbtjänsten för resultaten från riksdagsvalets gjordes en överbelastningsangrepp (på finska) https://yle.fi/uutiset/3-10731312
- Amerikanska NSA:s spionverktyg misstänks ha kommit i händerna på en kinesisk grupp (på engelska) https://www.nytimes.com/2019/05/06/us/politics/china-hacking-cyber.html

Maj

- Bluekeep-sårbarheten kan leda till en epidemi med skadliga program som sprider sig självständigt https://www.kyberturvallisuuskeskus.fi/sv/aktuellt/kritisk-sarbarhet-bluekeep-i-rds-tjansten-kraver-en-omedelbar-uppdatering-i-aldre-windows
- Big game hunting-grupperna utnyttjar allmänna skadliga program https://www.kyberturvallisuuskeskus.fi/sv/aktuellt/utnyttjade-sarbarheter-fordystrade-cybervadret-i-maj

Juni

- Varning 01/2019: Dataintrång genom en sårbarhet i e-postservern Exim https://www.kyberturvallisuuskeskus.fi/sv/dataintrang-genom-en-sarbarhet-i-e-postservern-exim
- Kommunfall: Lahtis (på finska) https://www.tivi.fi/uutiset/kyberhyokkays-sekoitti-lahden-jarjestelmat-vakavat-hairiot-jatkuvat/30bfba87-5e49-461a-9443-4389ddb349e5

Juli

- Störning i Galileo, tjänsten ur bruk en vecka (på finska) https://www.tekniikkatalous.fi/uutiset/undefined/ffb69bba-167a-4bae-b654-2ef46cc7c03b
- Kommunfall: Kumo (på finska) https://yle.fi/uutiset/3-10899982

Augusti

- Statsförvaltningens webbplats föremål för överbelastningsangrepp (på finska) https://yle.fi/uutiset/3-10933059
- Varning 02/2019: Sårbarheten i Microsofts fjärrskrivbordstjänst RDS används för dataintrång https://www.kyberturvallisuuskeskus.fi/sv/sarbarheten-i-microsofts-fjarrskrivbordstjanst-rds-anvands-dataintrang
- Kommunfall: Björneborg (på finska) https://yle.fi/uutiset/3-10913191

September

- Varningen om nätfiske av Office 365-koder har slopats https://www.kyberturvallisuuskeskus.fi/sv/aktuellt/varning-en-om-natfiske-av-office-365-koder-har-slopats
- Cyberbrottslingar har gripits i internationella operationer (på engelska) https://www.fbi.gov/news/stories/operation-rewired-bec-takedown-091019

Oktober

- På 15 år har IoT-apparaternas datasäkerhet inte förbättrats (på engelska) https://cyber-itl.org/2019/08/26/iot-data-writeup.html
- Allmänt spritt fynd i nätverksdiskar som gäller skadliga programmet QSnatch https://www.kyberturvallisuuskeskus.fi/sv/aktuellt/qsnatch-skadligt-program-mot-qnap-nas-enheter
- De som spionerar efter uppfinningar samlar också information om personer (på engelska) https://www.zdnet.com/article/iranian-hackers-credential-stealing-phishing-attacks-against-universities-around-the-world/
- Utomstående utnyttjas i överbelastningsangreppstrafikens spegling på det egentliga objektet https://www.kyberturvallisuuskeskus.fi/sv/ajankohtaista/2019-lokakuun-kybersaa

November

- Cybersäkerhetsmärket hjälper konsumenterna att göra säkrare anskaffningar av smarta apparater i hemmet - Finland först i Europa med att säkerställa säkerheten för smarta apparater https://tietoturvamerkki.fi/sv
- En identifiering i flera skeden skulle förebygga största delen av dataintrången i Office 365 (på engelska) https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-mfa-get-started

December

- Vår årliga kartläggning avslöjade än en gång över 1 000 oskyddade apparater i inhemska datanät https://www.kyberturvallisuuskeskus.fi/sv/aktuellt/lite-over-tusen-oskyddade-automationsenheter-i-finland-ska-nat
- Ibruktagandet av DNSSEC-datasäkerhetsutvidgningen fick en bra start https://www.kyberturvallisuuskeskus.fi/sv/aktuellt/anvandning-av-sakerhetstillagget-dnssec-tog-ett-stort-steg-framat-i-finland-digitala

Behöver du eller din organisation hjälp med att bekämpa kränkningar av informationssäkerheten eller har du frågor om lagstiftningen om cybersäkerhet? Vi utvärderar och godkänner även informationssystem.

Vi utvecklar och övervakar kommunikationsnätens och -tjänsternas driftssäkerhet och trygghet.
Du når oss:

per e-post: cert@traficom.fi
via kundtjänsten: 0295 345 630

Följ oss och våra nyheter
https://www.kyberturvallisuuskeskus.fi/sv/@CERTFI
https://www.facebook.com/NCSC.FI/

Anmäl kränkningar av informationssäkerheten till oss
https://www.kyberturvallisuuskeskus.fi/sv/anmal

Transport- och kommunikationsverket Traficom
Cybersäkerhetscentret

PB 320, 00059 TRAFICOM
tfn 029 534 5000

kyberturvallisuuskeskus.fi

ISNN 2669-8757 (webbpublikation)

TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret