Informationssäkerhetens år 2021

Cybersäkerheten i en tid av tillväxt – vi förhindrar störningar i förväg

Cybersäkerhetscentrets årsöversikt

Traficoms publikationer
3/2022

TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret

Innehållsförteckning

Cybersäkerheten passerade tonåren

År 2021 präglades vår vardag av flera informationssäkerhets- och cyberstörningar. Bland annat nätfiskebedrägerier efter nätbankskoder kom möjligtvis för att stanna. I fjol förlorade finländarna tiotals miljoner euro till brottslingar till följd av bedrägerier.

Nästan alla stiftade bekantskap med sms som spred skadeprogrammet FluBot med hjälp av olika teman. Skadeprogrammet var inte enbart förargligt, utan offren förlorade uppgifter och pengar. Angripna enheter sprider också skadeprogrammet vidare.

Vem som helst kan falla offer för ett bedrägeri. Var och en av oss kan hjälpa sina närstående genom att sprida information om bedrägerier.

Cyberstörningar som påverkade vardagen förekom runt om i världen. Det är bra att komma ihåg att cyberstörningar inte håller sig inom ländernas gränser och att konsekvenserna kan sträcka sig även till Finland. Till exempel i vårt grannland Sverige blev dagligvarukedjan Coop tvungen att stänga sina butiker på grund av ett cyberangrepp.

Eftersom allt fler människors vardag berörs av informationssäkerhet och cybersäkerhet, letar även vi på Cybersäkerhetscentret efter kommunikationskanaler som når så många som möjligt. I slutet av året började vi informera om omfattande informationssäkerhetsstörningar som berör finländarna i appen 112 Suomi.

Fokus för vår verksamhet ligger allt mer på att förebygga allvarliga cyberstörningar. Det här arbetet har underlättats av att allt fler känner till Cybersäkerhetscentret och våra fantastiska sakkunniga. Antalet informationssäkerhetincidenter som vi hanterar ökar från år till år. År 2021 hanterade vi tiotusentals informationssäkerhetsincidenter. Tack vare dem kunde en enorm mängd problem undvikas innan de blev allvarligare. Antalet allvarliga felsituationer i näten i Finland fortsatte att minska på lång sikt. Aktörerna som ansvarar för de finländska näten och regleringen som stöder dem är därför helt klart på rätt spår. När det gäller antalet incidenter ligger nätfiske fortfarande i topp. Även styrkorna på överbelastningsangreppen ökade.

Vi arbetade förebyggande även genom att uppdatera föreskrifter och bereda rekommendationer i samarbete med teleoperatörerna. Arbetet fortsätter bland annat inom ramarna för Utvecklingsprogrammet för cybersäkerheten som publicerades år 2021. Erkännandet Vägvisare för informationssäkerheten tilldelades LokalTapiola för bolagets satsningar på förebyggande verksamhet.

”Cyberstörningar har 2021 blivit en del av den nya normala vardagen.

Även på regleringsfronten hände det mycket. Statsrådets fattade ett principbeslut om förbättring av informationssäkerheten och dataskyddet inom kritiska samhällssektorer (Titukri). Man vill föreskriva lagstadgade informationssäkerhetskrav för alla kritiska sektorer, och kritiska informationssystem ska utvärderas i större utsträckning än i dag. Under året bereddes ny reglering om cybersäkerhet i anknytning till EU:s direktiv om nät- och informationssäkerhet (NIS 2). Även i EU:s kommande rättsakt om artificiell intelligens kommer cybersäkerhetsfrågor att uppmärksammas.

Även festligheter hörde till året 2021, då 20-årsjubileet för vår CERT-verksamhet närmade sig. Officiellt grundades CERT-FI i januari 2002. Finland har länge redan varit en föregångare inom informationssäkerhet och cybersäkerhet, och vi antar denna utmaning även år 2022.

Året innehöll även många utmaningar i fråga om resurser, och cybersäkerheten lider ännu av växtvärk. Året kan dock sammanfattas genom att konstatera att cybersäkerheten har passerat tonåren. Vi är starkare än tidigare när vi möter nya och ännu större utmaningar.

Sauli Pahlman
överdirektör
Cybersäkerhetscentret

Nyckeltal för vår verksamhet

2021 2020

Oavbruten jour

Behandlade fall

Varningar

Nedkörningar av skadliga webbplatser

Fall som behandlats av sårbarhetskoordineringen

Autoreporter

Kontakttillfällen från media

Facebook-följare

Twitter-följare

Antalet störningar

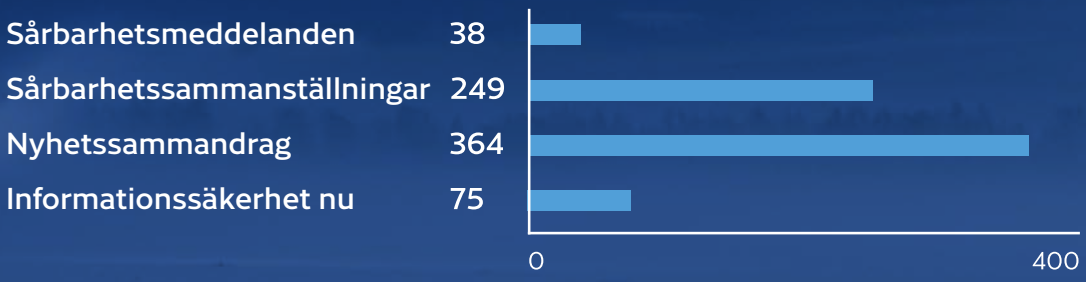
Kritiska störningar

Allvarliga störningar

Betydande störningar

Alla störningar totalt

Kommunikation och meddelanden



Enkäter om kundnöjdhet

Under året genomförde vi enkäter om kundnöjdhet i fråga om våra lägesbildsprodukter och våra grupper för informationsutbyte. Skalan för bedömningen i våra enkäter var från dåligt (1) till utmärkt (5). Medeltalet för nöjdheten var i båda enkäterna 4,3.

Enligt en enkät om lägesbilden används våra lägesbildsprodukter för att upprätthålla organisationens informationssäkerhet samt för att ge information om nya sårbarheter och aktuella incidenter. Cybersäkerhetscentret sammanställer lägesbilden med hjälp av uppgifter från flera olika källor och förmedlar den vidare via olika produkter.

ISAC-samarbetet producerar information som Cybersäkerhetscentrets kan använda för att bygga upp och utöka lägesbilden. Genom samarbetet har man även kunnat förhindra informationssäkerhetsavvikelser.

Bland våra lägesbildsprodukter är de mest lästa:

- Cyberväder
- varningar
- sårbarhetsmeddelanden
- veckorapporter

Grupperna för informationsutbyte (ISAC) uppskattade särskilt att

- man öppet utbyter information i grupperna inom förtroendenätet
- man i grupperna får information som står utanför den offentliga informationsförmedlingen
- ISAC-grupperna är ett effektivt och neutralt sätt för kontakt och informationsutbyte mellan myndigheten och verksamhetsfältet.

Lägesbildsprodukter

4,2 (2020) 4,3 (2021)

Medeltal

Verksamhetsfältsspecifika grupper för informationsutbyte

4,4 (2020) 4,3 (2021)

Medeltal

Hur påverkade vi?

Den digitala utvecklingen ger oss kontinuerligt tillgång till nya tjänster, förbättrar och underlättar vår vardag och vårt liv samt skapar nya lösningar som vi kan använda för att lösa globala utmaningar. Även om denna utveckling i huvudsak för gott med sig, är nackdelarna med den digitala utvecklingen en ständigt ökande cyberbrottslighet samt olika störningar.

Liksom alla digitala fenomen karakteriseras även cyberhot av en snabb utveckling. Fenomen med anknytning till cybersäkerhet är ofta även komplicerade och följer inte i förväg fastställda myndighetsansvar. Detta förutsätter en ny slags funktions- och reaktionsförmåga även av myndigheterna.

En av Cybersäkerhetscentrets fördelar är ett omfattande verksamhetsfält samt en mångsidig teknisk, juridisk och samhällelig kompetens till stöd för detta. Med hjälp av dessa kan vi vid behov organisera oss även mycket snabbt i samarbete med våra nationella och internationella samarbetspartner för att svara på olika situationer och behov.

Utvecklingsprogrammet och Titukri-utvecklingen som drivkraft

För att förbättra cybersäkerheten togs olika initiativ. De viktigaste av dessa var det nationella utvecklingsprogrammet för cybersäkerheten och statsrådets principbeslut om förbättring av informationssäkerheten och dataskyddet inom kritiska samhällssektorer (Titukri). Inom utvecklingsprogrammet förbättras cybersäkerheten på lång sikt, över sektorsgränserna. Titukri sätter fart på förbättringen av nivån på informationssäkerheten och dataskyddet i samhällets kritiska informationssystem.

Utvecklingsprogrammet för cybersäkerheten upprättades år 2021 och inom det definieras viktiga åtgärder för att förbättra cybersäkerheten i hela samhället.

Utvecklingsprogrammet utarbetades genom ett omfattande samarbete och sträcker sig ända till år 2030. Det främsta målet för programmet är att skapa ett ekosystem för cybersäkerhet i Finland som genererar livskraft och tillväxt, ökar antalet arbetsplatser inom branschen, skapar nödvändig kompetens samt förbättrar det digitala samhällets hållbarhet och tålighet i förhållande till olika fenomen i cybermiljön. Utvecklingsprogrammet är uppbyggt kring fyra huvudteman: **högklassig kompetens, nära samarbete, en stark finländsk cybersäkerhetsindustri** och **effektiva nationella cybersäkerhetskapaciteter.** Det är uppenbart att en stark nationell cybersäkerhet förutsätter nödvändig kompetens på alla nivåer i samhället.

På myndighetsnivå har Cybersäkerhetscentret en viktig roll när det gäller att utveckla kompetensen hos såväl myndigheter och företag som vanliga medborgare.

För att stärka ekosystemet för cybersäkerhet krävs att samarbetet stärks på lång sikt.

Cybersäkerhetscentret har en viktig roll i fråga om utvecklingen av samarbetet på både nationell och internationell nivå. Ett av de viktigaste verktygen som identifierats för utvecklingen av samarbetet är övningsverksamhet som gäller cybersäkerhet.

När det gäller en stark inhemsk cybersäkerhetsindustri bör särskild uppmärksamhet ägnas åt kompetenscentrumet för cybersäkerhet som EU kommer att inrätta samt nätverket av nationella samordningscentrum. Transport- och kommunikationsverkets Cybersäkerhetscenter har utsetts till nationellt samordningscentrum, och genom denna roll strävar centret efter att stödja den nationella cybersäkerhetsmarknaden och -industrin i den allt hårdare internationella konkurrensen. Det sista huvudtemat för utvecklingsprogrammet gäller effektivisering av de nationella cybersäkerhetskapaciteterna. Dessa kapaciteter skapar en grund för hela samhällets verksamhet och säkerhet samt främjar vår suveränitet i cybermiljön.

”Det främsta målet för utvecklingsprogrammet är att skapa ett ekosystem för cybersäkerhet i Finland.

Titukri bidrar till att framöver bekämpa händelser i likhet med Vastaamo

Till följd av dataintrånget mot Vastaamo utarbetade statsrådet under år 2021 ett principbeslut om förbättring av informationssäkerheten och dataskyddet inom kritiska samhällssektorer. För att målen i principbeslutet ska kunna uppfyllas spelar vi en viktig roll i detta arbete. I principbeslutet har uppmärksamhet särskilt ägnats åt ett ännu effektivare och mer organiserat samarbete mellan myndigheterna, bindande informationssäkerhetskrav, regelbunden övervakning av kraven, identifiering av kritiska processer och funktioner samt utvärdering och revision av informationssystem. Cybersäkerhetscentret har en nyckelroll i främjandet av målen för principbeslutet, utvecklingen av samarbetet i fråga om cybersäkerhet och stödjandet av andra myndigheters verksamhet. Det är uppenbart att Cybersäkerhetscentrets resurser bör stärkas, så att det kan stödja och ge övriga sektorer ännu mer sådan sektorspecifik rådgivning och sådant sektorspecifikt stöd som identifierats i arbetet med principbeslutet.

Även om man försöker främja användningen av Cybersäkerhetscentrets stödåtgärder och de tjänster som det producerar inom olika sektorer, bör varje sektor fortsätta att utveckla sin verksamhet så att den genomförs på ett sådant sätt att informationssäkerheten säkerställs i ännu högre grad. Utgångspunkten bör vara att informationssäkerheten är integrerad i verksamhetskulturen i de kritiska sektorerna och aktörerna måste själva ansvara för detta.

”Informationssäkerheten borde vara integrerad i verksamhetskulturen i de kritiska sektorerna.

Nätbedragare krossas med gemensamma krafter

Vem som helst kan falla offer för nätbedrägerier, och kriminella har kommit över tiotals miljoner euro i samband med sådana. För att bekämpa bedrägerier bedriver myndigheter, företag och organisationer ett omfattande samarbete. År 2021 fick man för första gången information om cyberstörningar direkt i mobilen via appen 112 Suomi.

Finländarna förlorar tiotals miljoner euro varje år till följd av olika typer av nätbedrägerier. Cybersäkerhetscentret samarbetar aktivt med teleoperatörer, polisen samt övriga myndigheter och organisationer för att förebygga nätbedrägerier. Cybersäkerhetscentrets meddelanden och varningar ger aktuell och exakt information om hurdana bedrägerier och nätfiskekampanjer som pågår. Bedrägerikampanjer som genomförs av kriminella handlar inte om något småpysslande eller sådant som hackare ägnar sig åt, utan de genomförs av internationella proffsligor. Enbart informering från myndigheternas sida löser inte problemet, utan för att upplysa finländarna måste hela mediefältet delta, från kvällstidningarna till morgonnyheterna. Vi har pressen att tacka för att bedrägerifenomen kommer till allmänhetens kännedom. Cybersäkerhetscentret deltar även i Konsumentförbundets projekt för att få bukt med bedragare (Huijarit kuriin!) som syftar till aktivt upplysningsarbete för att förhindra bedrägerier.

Som ny kommunikationskanal har Cybersäkerhetscentret fått appen 112 Suomi, som lanserats av Nödcentralsverket och som används av nästan två miljoner finländare. Under år 2021 utfärdades varningar om omfattande bedrägerikampanjer mot privatpersoner via appen 112 Suomi vid två tillfällen. Miljontals finländare har varnats om farliga bedrägerier och skadeprogram, men ändå kommer det hela tiden nya offer. Målet är att under de kommande åren kunna minska antalet offer och den brottsliga vinningen.

”Enbart informering från myndigheternas sida löser inte problemet, utan för att upplysa finländarna måste hela mediefältet delta, från kvällstidningarna till morgonnyheterna.

Traficom och teleoperatörerna bekämpar tillsammans bedrägerisamtal och skadeprogram som sprids via sms

För att få bukt med vissa bedrägerier behövs åtgärder av teleoperatörerna. År 2021 letade teleoperatörerna och Traficom tillsammans efter olika sätt att förhindra förfalskning av telefonnummer. När skadeprogrammet FluBot förhindrades hamnade över en miljon skadliga meddelanden i operatörernas meddelandefilter.

Att förfalska uppringarens telefonnummer till ett finländskt telefonnummer är en teknik som i stor utsträckning används av internationella brottslingar och som gör att finländska offer med mycket större sannolikhet litar och svarar på bedrägerisamtal från utlandet samt till exempel ger sina nätbankskoder eller överlåter sin dator för fjärrstyrning av brottslingarna.

Förfalskning av utländska uppringares telefonnummer vid bedrägerisamtal har sedan i fjol varit ett stort problem även i Finland. För att motverka situationen började Traficom tillsammans med teleoperatörerna utarbeta olika metoder för att förhindra förfalskning av uppringares telefonnummer till finländska nummer. Målet är att försvåra och förhindra verksamheten för internationella brottslingar. Tack vare lösningen kan teleoperatören se till att ett nummer hör till en abonnent som har rätt att använda numret i fråga. Samtalets mottagare kan i sin tur lita på att samtal från ett finländskt nummer rings från ett finländskt telefonabonnemang.

Dessutom kan den som har ett finländskt telefonabonnemang och ett finländskt nummer lita på att hans eller hennes telefonnummer inte används för brott.

Snabba åtgärder tillsammans med teleoperatörerna för att hindra spridning av skadeprogrammet FluBot

I samarbete med teleföretagen förhindrade vi spridningen av FluBot, ett skadeprogram som sprids i mobiler, som startade på sommaren. Vi förmedlade aktuell information till teleföretagen om vilka kommandokanaler programmet använde, så att företagen skulle kunna filtrera nättrafiken till dem. Detta gjorde skadeprogrammet funktionsodugligt och hindrade att det spreds vidare från angripna enheter.

I november började en ny och mer avancerad version av FluBot spridas som använde protokollet DNS Over HTTPS (DoH) som kommandokanal. Denna version kan inte bekämpas genom filtrering av nättrafiken, utan att flera andra tjänsters funktion störs. Vi kämpade mot den nya vågen av FluBot bland annat genom att rekommendera teleföretagen att filtrera de sms som spred skadeprogrammet. Över en miljon sms filtrerades, vilket betyder att åtgärden hade stor betydelse när det gällde att minska vidarespridningen.

Uppdatering av föreskriften om elektroniska identifieringstjänster och betrodda elektroniska tjänster i samarbete med verksamhetsfältet

Vi uppdaterade vår föreskrift om elektroniska identifieringstjänster och betrodda elektroniska tjänster. I den förnyade föreskriften föreskrivs bland annat

1. om obligatoriska kontroller som förbättrar säkerheten för slutanvändaren, såsom sessions-ID och verifierade uppgifter om måltjänsten
2. att användaren ska informeras på ett sammanhängande och bättre sätt under hela identifieringstransaktionen
3. om nya alternativ för att verifiera och trygga dataförbindelserna mellan olika aktörer
4. om uppdaterade och mer flexibla krav på krypteringsförfaranden, vilket till exempel gör det enklare att införa nya krypteringslösningar
5. att en separat riskbedömning ska göras om identifieringsmetoden där hoten mot och de skyddande åtgärderna för identifieringsmetoden och -faktorerna utvärderas.

Våra tjänster för näringslivet

Cybersäkerhetscentret utvecklar och producerar cybersäkerhetstjänster för näringslivet och aktörer som är kritiska för försörjningsberedskapen. Tjänsterna bidrar till att upprätthålla och utveckla informationssäkerheten i en snabbt föränderlig värld. De som använder Cybersäkerhetscentrets tjänster bildar ett informationssäkerhetssamfund, där information delas konfidentiellt.

Cybermätaren

Cybermätarens första år har kommit till sitt slut, och utifrån responsen vi fått finns det efterfrågan på en systematisk utvärderingsmodell för kapaciteterna i fråga om cybersäkerhet. Under året har Cybermätaren presenterats för intressenter, respons samlats in, utbildningar ordnats och nya idéer testats. I början av 2022 publiceras en ny version av Cybermätaren där kundresponsen har beaktats och även ändringarna enligt version 2 av modellen Cybersecurity Capability Maturity Model (C2M2) som publicerades under sommaren har implementerats.

ISAC-träning ger kunskaper till nytta för verksamhetsfälten

Under det gångna året 2021 har vi i samarbete med ISAC-aktörerna* utvecklat cyberträning för Cybersäkerhetscentrets grupper för informationsutbyte. Vi har ordnat träningstillfällen för ISAC-grupperna inom livsmedelsproduktion och -distribution, energi, vattentjänster samt logistik och transport i samarbete med Insta och Fraktal. Temat för träningarna har varit informationsutbyte, lägesbilden och myndigheternas roll vid omfattande cyberstörningar som berör verksamhetsfältet. Man har gjort goda observationer och fått kunskaper vid de gemensamma träningarna för ISAC-aktörerna som förbättrar de aktuella verksamhetsfältens beredskap och förmåga att möta cyberhot.

HAVARO

Observations- och varningssystemet för allvarliga informationssäkerhetsincidenter HAVARO förnyades år 2021. Tjänsten erbjuds nu i större utsträckning till finländska organisationer i samarbete med kommersiella informationssäkerhetsaktörer. Tietoturva ry tilldelade HAVARO erkännandet årets informationssäkerhetsprodukt.

* ISAC-grupperna för informationsutbyte (ISAC=Information Sharing and Analysis Centre) är samarbetsorgan kring cybersäkerhet som inrättats för olika branscher.

Tillförlitlig tids- och positionsinformation är samhällets stöttepelare

Samhället blir allt mer beroende av den positions- och tidsinformation som satellitnavigeringssystemen producerar. Syftet med en offentligt reglerad satellittjänst (Public Regulated Service, PRS) inom ramarna för det europeiska navigeringssystemet Galileo är att producera verifierad och kontinuerlig positions- och tidsinformation åt myndigheter och försörjningsberedskapskritiska företag under alla förhållanden.

De kommande användarna av PRS-tjänsten i Finland är till exempel polisen, Tullen, Försvarsmakten, räddningsväsendet, företag som är kritiska med tanke på försörjningsberedskapen, såsom teleföretag och banker, energisektorn samt transport- och logistikbranschen.

Samhällets stöttepelare – tillförlitlig tids- och positionsinformation – fick ett stadigt fotfäste i november 2020, då regeringens finanspolitiska ministerutskott fastställde att en PRS-tjänst ska införas i Finland år 2024. Vi började planerade tjänsten tillsammans med de kommande tjänsteoperatörerna Suomen Erillisverkot Oy och Försvarsmakten.

”Temat för träningarna har varit informationsutbyte, lägesbilden och myndigheternas roll vid omfattande cyberstörningar som berör verksamhetsfältet.

Kommunikationsnätens säkerhet

Vårt samhälle blir allt mer beroende av kommunikationsnät och nättekniken utvecklas. År 2021 funderade man i synnerhet över informationssäkerheten i 5G-näten och skyddet av nätens mest kritiska delar.

Kommunikationsnätens säkerhet har fortsättningsvis haft hög prioritet i diskussioner på såväl EU- som internationell nivå. Inom EU har medlemsstaterna aktivare än någonsin behandlat ibruktagandet av och säkerheten hos den senaste nätgenerationen 5G. Dessa diskussioner kommer även att fortsätta och deras betydelse att öka ytterligare i takt med att kommunikationsnätens teknik utvecklas och samhällets beroende av kommunikationsnät ökar. I början av 2021 trädde nya bestämmelser om kommunikationsnätens säkerhet i kraft i Finland.

På den nationella regleringen inverkade i synnerhet EU:s gemensamma förhållningssätt i fråga om att svara mot oron vad beträffar säkerheten i 5G-näten. EU:s gemensamma arbete för säkerheten i 5G-näten kulminerade i en uppsättning gemensamma instrument (toolbox) som kommissionen och medlemsstaterna utarbetat och där flera åtgärder för att säkerställa säkerheten i 5G-näten och de tjänster som fungerar med hjälp av dem lyfts fram.

En av de viktigaste åtgärderna bland instrumenten är att på ett tillräckligt sätt skydda nätets allra mest kritiska delar. I den nationella regleringen som trädde i kraft i början av året möjliggörs utvärdering av kommunikationsnätens kritiska delar med tanke på den nationella säkerheten och landets försvar. Utgångspunkten är att man i de kritiska delarna av ett kommunikationsnät inte får använda anordningar som kan äventyra den nationella säkerheten. Om en sådan anordning påträffas kan man förordna att den avlägsnas.

Den ovannämnda regleringen av säkerheten hos kommunikationsnätens kritiska delar kompletterades våren 2021 med en teknisk föreskrift utfärdad av Transport- och kommunikationsverket. Genom föreskriften förtydligades den tekniska definitionen och identifieringen av de kritiska delarna. Såväl den nationella regleringen som Transport- och kommunikationsverkets föreskrift upprättades genom ett omfattande tväradministrativt samarbete. Även representanter för verksamhetsfältet deltog aktivt i beredningsarbetet. I fråga om den utarbetade regleringen och i synnerhet den nya föreskriften är det skäl att komma ihåg att de verktyg som tas fram till följd av den tekniska utvecklingen även måste kunna uppdateras snabbt. Därför kommer den tekniska utvecklingen och de förändringsbehov den för med sig bland annat i fråga om reglering att utvärderas regelbundet i delegationen för nätsäkerhet som inrättades i början av 2021.

”En av de viktigaste åtgärderna bland instrumenten är att på ett tillräckligt sätt skydda nätets allra mest kritiska delar.

Cybervädерfenomen

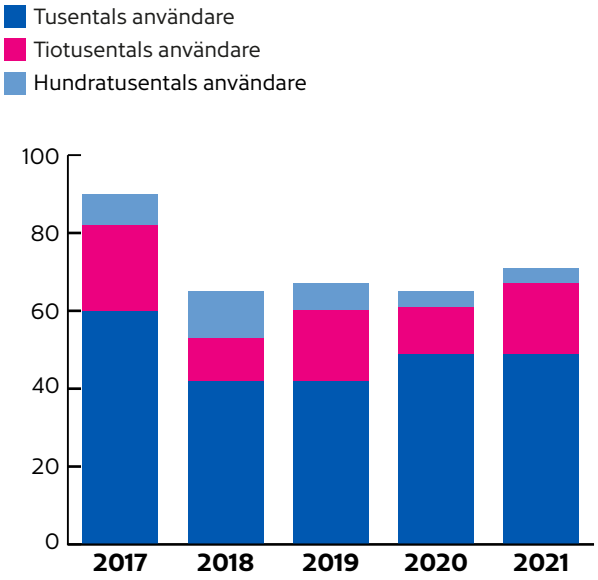
På cybervädерkartorna syntes kraftiga överbelastningsangrepp, aggressiva skadeprogram och en rekordstor mängd nätfiske.

Nätens funktion

Antalet allvarliga felsituationer i näten i Finland fortsatte att minska på lång sikt. Avbrott i globala tjänster märks även hos oss.

Störningar i kommunikationsnäten

År 2021 gjorde olika avbrott i det allmänna kommunikationsnätet och i internationella tjänster det än en gång tydligt för oss hur beroende vi är av fungerande förbindelser och olika digitala tjänster. Ett omfattande serviceavbrott kan ge konsekvenser i samhällets kritiska funktioner – samtidigt kan samma avbrott även hindra medborgarna från att använda sociala medier tills felet är åtgärdat. Vi är vana vid att tjänsterna ständigt är tillgängliga på nätet. Olika avbrott i det inhemska nätet, banktjänster eller sociala medier visar på ett konkret sätt att riskhantering och beredskap är viktiga även för tjänsternas användare. På grund av ett avbrott kanske dina inköp förblir obetalda, ett litet företags konto på sociala medier inte uppdateras eller så kan du inte se på film via en strömningstjänst.



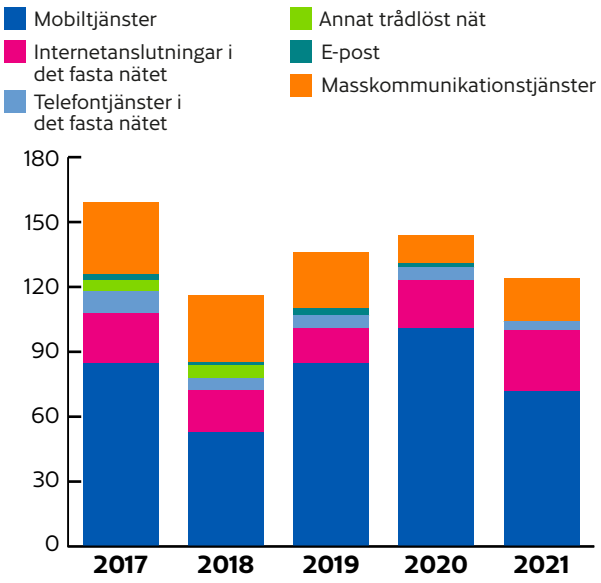
Antalet betydande funktionsstörningar i de allmänna kommunikationstjänsterna 2017–2021

”Utvecklingsriktningen kan anses vara positiv, även om antalet betydande störningar inte längre har minskat.

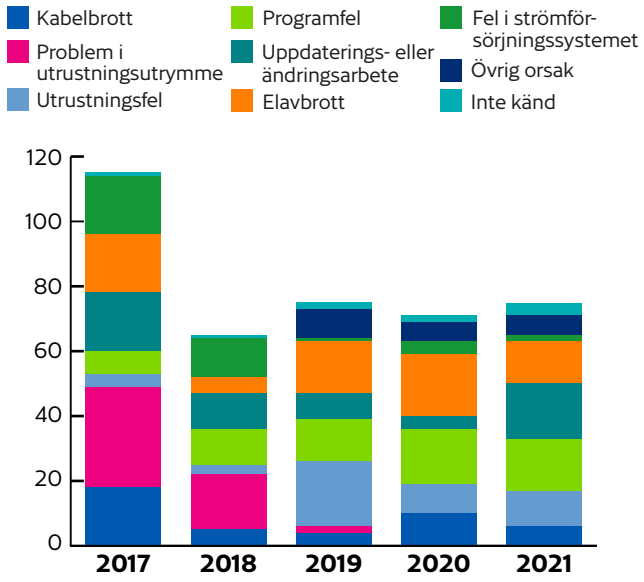
I Finland är läget för kommunikationsnäten fortfarande stabilt

Vi samlar information om störningar i de inhemska kommunikationsnäten. På så sätt kommer vi åt grundorsakerna till störningarna, vilket låter oss förbättra nätens säkerhet och funktionssäkerhet i samarbete med verksamhetsfältet.

Antalet betydande störningar minskade klart fram till år 2018. Efter det har det rapporterats 65–73 störningar årligen. År 2021 förekom det 73 betydande störningar. Kapaciteten i våra nät har varit fullt tillräcklig under hela pandemin och för den ökade belastningen.Antalet kritiska störningar som gäller åtminstone 100 000 användare har minskat de senaste åren. Som helhet kan utvecklingsriktningen anses vara positiv, även om antalet betydande störningar inte längre har minskat.



Konsekvenserna av betydande funktionsstörningar på allmänna kommunikationstjänster 2017–2021. En störning kan inverka på flera tjänster.



Grundorsaker till betydande funktionsstörningar 2017–2021. En störning kan ha flera grundorsaker.

”Avbrotten påminner oss om att vilken tjänst som helst kan avbrytas när som helst.

Majoriteten av de betydande störningarna i de inhemska kommunikationsnäten gäller tjänster i mobilnäten, det vill säga funktionen hos samtal, internetanslutningar och textmeddelanden.

Till exempel elavbrott, olika konfigurationsfel, utrustningsfel och kabelbrott orsakar fel i nätet. Orsaken till felet kan även vara ett mänskligt skrivfel eller en grävmaskinsskopa som kapat en kabel. Teleföretagen blev föremål även för överbelastningsangrepp och till exempel namnservrar angreps år 2021. Angreppen fick dock inga stora konsekvenser.

De stora stormarna som drabbade Finland i slutet av juni år 2021 fick namnen Aatu och Paula. I juni rapporterades också 14 stora störningar i tjänster i det allmänna kommunikationsnätet till Cybersäkerhetscentret. I juli orsakade en grävmaskin ett brott på en fiberkabel, vilket inverkade på Valtoris olika tjänster i flera timmar. Ett fungerande samarbete mellan myndigheter, teleoperatörer och elbolag främjar beredskapen för stormar och olika avvikande situationer.

Problem i populära och globala tjänster märktes även hos oss

Det blev avbrott i e-posttjänster i synnerhet i mars på grund av sårbarheten hos Microsoft Exchanges e-postservrar. Uppdateringar för att åtgärda sårbarheten och utredningar av informationssäkerheten i servrarna gjorde att e-posttrafiken stundtals var lugn på sina håll. En betydande sårbarhet orsakade åtminstone tillfälligt avbrott i e-posttrafiken, när servrarna måste uppdateras så fort som möjligt på grund av allvarlighetsgraden – till och med mitt under arbetsdagen.

I september ledde ett världsomfattande serviceavbrott i Facebook, WhatsApp och Instagram till att användningen av tjänsterna avbröts för flera timmar under en vardagskväll. Även till exempel Microsofts, Slacks, Salesforces och Fastlys tjänster fungerade bristfälligt under året. Avbrotten märktes i tillgången till tjänsterna och till exempel i form av att olika webbplatser inte fungerade. Enligt de internationella tjänsteleverantörerna orsakades problemen av bland annat olika konfigurationsfel eller planeringsfel i apparna. Avbrotten påminner oss om att vilken tjänst som helst kan avbrytas när som helst. Medborgarna och organisationerna bör även vara medvetna om att tjänster på sociala medier ibland kan vara otillgängliga även under längre perioder. Vi är vana vid god tillgång till tjänster, men exemplen visar att avbrott kan ha förargliga konsekvenser för till exempel uppdateringar av små och medelstora företags reklamsidor eller medborgarnas kontakt med sina närstående.

Anmälningarna om personuppgiftsincidenter har minskat

Antalet anmälningar från teleföretagen om informationssäkerhetsincidenter som gäller personuppgifter har minskat i jämn takt sedan toppen år 2018. Ett typiskt exempel är att ett teleföretag skickar ett brev eller ett e-postmeddelande med en kunds personuppgifter till fel adress. Vanligtvis inträffar det färre än tio betydande informationssäkerhetsincidenter per år. År 2021 anmäldes 17 sådana.

Överbelastningsangrepp

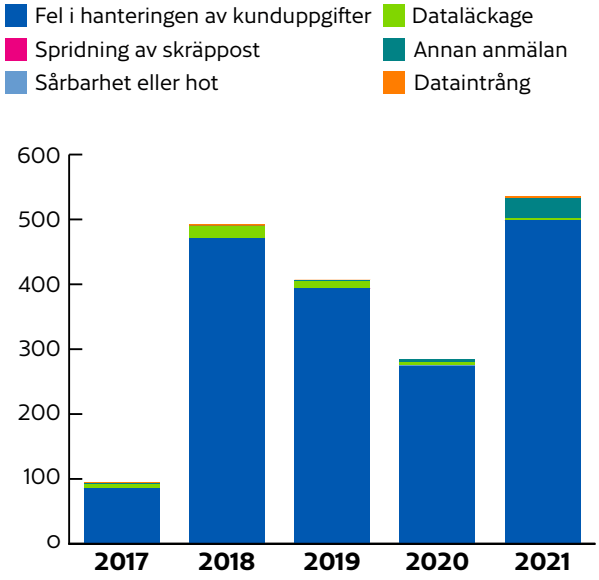
Cybersäkerhetscentret tog emot tiotals anmälningar om överbelastningsangrepp som påverkade organisationers funktionsförmåga. Angreppen orsakade antingen korta avbrott i till exempel de anställdas distansförbindelser eller så var de angrepp mot till exempel en nättjänst som pågick i flera timmar.

När de upprepas kan också korta överbelastningsangrepp vara ett gissel för en organisation om de indirekt orsakar problem i funktionen hos interna tjänster. Vi har fått flera anmälningar där ett angrepp har påverkat organisationens VPN-anslutningar.

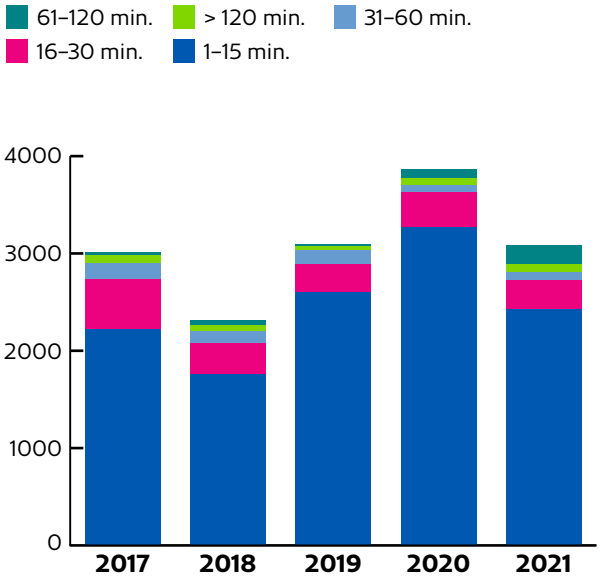
I sådana fall kan arbetet tillfälligt avbrytas och distansmöten får vänta tills förbindelserna har återställts. Ofta flyttar organisationer sina tjänster till molntjänster som har utvecklats för att tåla även stora överbelastningsangrepp så att sådana inte påverkar tjänsternas användbarhet.

I kommunerna riktades angrepp mot skolornas elektroniska tjänster

Från kommuner fick vi anmälningar om angrepp mot olika studietjänster för skolor eller skolors adresser i långdistansnätverk. Det är värt att planera tjänsterna så att inte ens kortvariga överbelastningsangrepp kan påverka deras funktion. Även polisen får varje år ta emot brottsanmälningar om överbelastningsangrepp. Korta angrepp kan orsaka avbrott i tjänster och ge upphov till exempelvis en utredningsprocess hos polisen. Det är bra att komma ihåg att även personer under 15 år kan ställas till svars för sådana. Vi uppmuntrar organisationer att göra brottsanmälningar om överbelastningsangrepp.



Telebolagens anmälningar om betydande informationssäkerhetsincidenter och personuppgiftsincidenter 2017–2021. År 2021 började fler telebolag anmäla incidenter, vilket gör att antalet verkar större än tidigare.



Utvecklingen för överbelastningsangreppens varaktighet i Finland. Källa: Telia

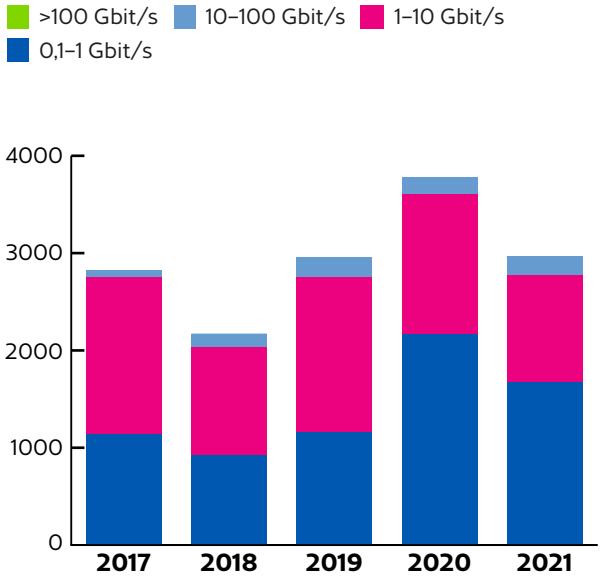
Överbelastningsangreppens volymer slog nya rekord

Under det gångna året stödde vi flera organisationer när överbelastningsangrepp inträffade och kompletterade lägesbilden över angreppen i samarbete med våra internationella samarbetspartner. I Finland är volymen på de överbelastningsangrepp som anmäls till Cybersäkerhetscentret vanligtvis omkring 1–10 Gbit/s. Inhemska organisationer är förberedda för angrepp av den här volymen, till exempel med hjälp av operatörernas tjänster för att mitigera konsekvenserna av angrepp.

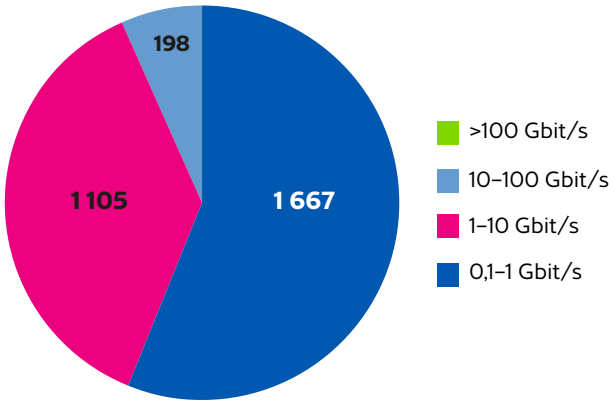
År 2021 upptäcktes en handfull massiva angrepp på omkring 100 Gbit/s i Finland, vilka orsakade bland annat serviceavbrott för olika organisationer. Vi fick även en anmälan om det största överbelastningsangreppet hittills i Finland. Angreppet på 260 Gbit/s var rekordstort, men tjänsterna för att mitigera konsekvenserna av angrepp lyckades förhindra det.

Även år 2021 utsattes inhemska organisationer för överbelastningsangrepp som inkluderade utpressningsmeddelanden. I några fall hittades utpressningsmeddelandet i e-postens skräpkorg, medan andra hade fått ett meddelande i samband med ett demonstrationsangrepp. De större angrepp som man hotade med genomfördes dock aldrig.

Demonstrationsangrepp kan mycket väl ha en volym på över 10 Gbit/s. Ute i världen har utpressningsmeddelanden skickats till exempel till teleoperatörer. Därtill berättade stora internationella tjänsteleverantörer återigen om rekordstora överbelastningsangrepp mot till exempel molntjänster. Molntjänster är dock planerade för att kunna stå emot olika typer av angrepp och ofta syns effekterna inte i tjänsternas funktion.



Utvecklingen för överbelastningsangreppens volymer i Finland.
Källa: Telia



Fördelningen av överbelastningsangreppens volymer i Finland 2021.
Källa: Telia

”Angreppet på 260 Gbit/s var rekordstort, men tjänsterna för att mitigera konsekvenserna av angrepp lyckades förhindra det.

Cyberspionage

Sårbara nätenheter och -tjänster är intressanta inom cyberspionage, eftersom man genom att utnyttja dem kan få tillgång till konfidentiell information, kommunikation eller olika system.

Cyberspionage har bedrivits aktivt även år 2021, men Finland har besparats de största stormarna. Strävan efter att utnyttja olika sårbarheter inom cyberspionageoperationer har synts i betydande utsträckning både i den offentliga debatten och i observationer med anknytning till cyberspionage. Även den ökade användningen av distansförbindelser till följd av att distansarbete blivit vanligare har förblivit ett lämpligt mål för cyberspionage.

Sårbara nätenheter som mål

Finländska organisationer är ständigt föremål för verksamhet som syftar till att hitta olika sårbara tjänster eller svaga lösenord, och detta har fortsatt även år 2021. En del av verksamheten tyder på illvillig verksamhet av statliga aktörer utifrån offentliga, kommersiella eller andra källor.

Föremål för aktivitet för att gissa lösenord är vanligtvis olika organisationers molntjänster eller tjänster som på annat sätt är tillgängliga via nätet.

Sårbara nätenheter och -tjänster är av intresse inom cyberspionage, eftersom de kan ge tillgång till konfidentiell information och kommunikation eller andra system. Sådana enheter och tjänster är å ena sidan till exempel e-postservrar, såsom Microsoft Exchange, och å andra sidan VPN-lösningar, såsom Pulse Connect Secure. I båda exemplen uppdagades sårbarheter under år 2021 som varit en metod för utnyttjande av även statliga cyberaktörer.

Sårbara små routrar och hemmaroutrar i Finland kan i sin tur utnyttjas som en del av cyberspionernas angreppsinfrastruktur.

Angrepp mot nätenheter och sårbara tjänster samt åtgärder för att hitta och utnyttja dessa bedöms fortsätta även nästa år.

”En del av verksamheten tyder på illvillig verksamhet av statliga aktörer utifrån offentliga, kommersiella eller andra källor.

Flera grupper har synts även i Finland

Olika APT-grupper riktar sitt intresse mot både finländska företag och den offentliga förvaltningen.

Även i Finland märktes till exempel den kampanj som skapade rubriker under våren och som i offentligheten tillskrevs gruppen NOBELIUM.

Kampanjen syntes i flera europeiska länder och inom den skickade gruppen, som även är känd under namnen APT29 och Cozy Bear, nätfiskemeddelanden eller meddelanden med skadliga bilagor till målorganisationer.

Samma gruppering påstås även ligga bakom den skadliga ändringen i SolarWinds administrationsverktyg Orion som upptäcktes i slutet av 2020. Grupperingen anklagas även för dataintrång i flera it-servicebolag på olika håll i världen år 2021.

Angrepp mot leveranskedjor förväntas orsaka omfattande utredningar även år 2022, när organisationer är tvungna att undersöka huruvida någon har försökt ta sig in i deras system via något annat företag eller system eller någon annan tjänst som hackats.

På våren tillskrev även Skyddspolisen cyberspionageincidenten mot riksdagen i slutet av 2020 APT31-operationen. Riksdagen berättade om cyberangreppet mot den vid årsskiftet 2020–2021 som påverkade en del av riksdagens e-postkonton. Utrikesministeriets personal hade man i sin tur försökt spionera på med hjälp av verktyget Pegasus, som är avsett för spionage mot mobila enheter. Användningen av det inom cyberspionage ledde till stora debatter sommaren 2021.

Cybersäkerhetscentret ger råd, informerar och utreder

Cybersäkerhetscentret följer aktivt utvecklingen när det gäller cyberspionageoperationer, ger akt på hot och informerar finländska organisationer om dem, på såväl ett generellt som individuellt plan. Cybersäkerhetscentret erbjuder hjälp till aktörer som misstänker att de blivit föremål för ett försök till cyberspionage eller något annat allvarligt dataintrång eller ett försök till ett sådant. Stödet kan inkludera till exempel rådgivning, en teknisk analys eller samordning av utredningen av dataintrånget.

Dessutom samarbetar Cybersäkerhetscentret med flera olika parter både nationellt och internationellt med målet att upprätthålla en aktuell lägesbild samt säkerställa att vi i Finland kan förbereda oss i förväg på olika slags utvecklingar och hot.

Skadeprogram och sårbarheter

När det gäller sårbarheter och skadeprogram dominerades året av den kritiska sårbarheten i e-postservern Microsoft Exchange och sårbarheten i komponenten Log4j samt skadeprogrammet FluBot, som spreds via sms.

Sårbarheten i Exchange fick fart på cyberbrottslingarna och krävde en varning

På våren rapporterades det i Finland och ute i världen om aktivt utnyttjande av en kritisk sårbarhet i e-postservern Exchange. Efter att sårbarheten läckte ut utnyttjades den snabbt allt mer i synnerhet bland cyberbrottslingar och statliga cyberaktörer.

Vi uppmuntrade och vägledde organisationer när det gällde att börja utreda dataintrång. I våra instruktioner betonade vi framför allt att det inte räckte med endast en programvaruuppdatering för att hålla angriparen på avstånd. Vi utfärdade även en varning om sårbarheten i januari 2021.

Till en början upptäckte vi i Finland cirka 300 sårbara Exchange-servrar, varav en del redan hade hackats. Det är viktigt att göra allmänheten medveten om sådana sårbarhetshelheter, så att utnyttjande av sårbarheten kan förhindras eller åtminstone upptäckas snabbt. Vi kontaktade över 250 organisationer, fram till slutet av mars hade vi fått information om 74 intrång. I början av april hade de finländska organisationernas sårbara Exchange-servrar uppdaterats.

Många anmälningar om skadeprogram för Android – FluBot i topp

På basis av de anmälningar om informationssäkerhetsincidenter vi fått var olika skadeprogram för operativsystemet Android temat för år 2021. Under året fick vi över 15 400 anmälningar, varav över 5 400 handlade om skadeprogram för Android. Särskilt många anmälningar om informationssäkerhetsincidenter handlade om skadeprogrammen FakeCop/FakeSpy och FluBot.

Den andra och den fjärde varningen som vi utfärdade under året handlade om FluBot. Under året försökte man sprida detta skadeprogram för Android med hjälp av till exempel sms som skickades i olika transporttjänsters namn. I juni blev det vanligare med sms som sade att mottagaren fått ett meddelande. I november var temat för sms:en ljudmeddelanden och paketleveranser. Enligt våra uppgifter skickades bluffmeddelanden på finska till tusentals finländare.

FluBot kan stjäla uppgifter i till exempel smarttelefoner samt från dem skicka bluffmeddelanden som sprider skadeprogrammet och även andra sms till utlandet. Försök att sprida skadeprogrammet kan gälla vilken enhet som helst, så förebyggande är därför viktigt. Det är bra i synnerhet för företag att veta vilka uppgifter som finns i de anställdas telefoner och att göra en riskbedömning av hurdana konsekvenser ett dataläckage till följd av ett skadeprogram skulle kunna ha.

Sårbarhet i Log4shell fördystrade slutet av året

Sårbarheten i biblioteket Lo4j som upptäcktes i början av december 2021 utnyttjades aktivt, och dataintrång i anslutning till den har inträffat även i Finland.

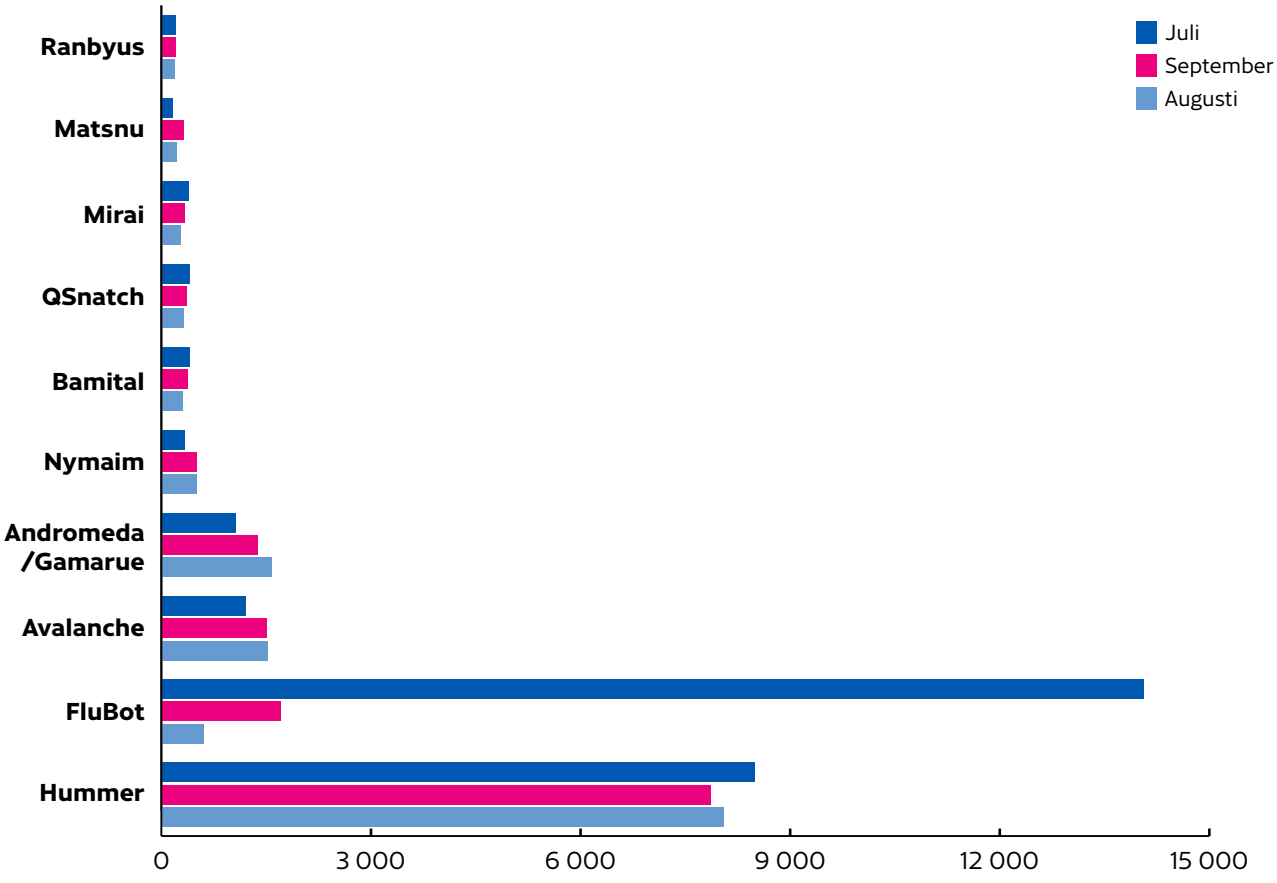
Vi utfärdade den sista kritiska varningen för 2021 om denna sårbarhet i maj 2021. Det som gör sårbarheten exceptionell är att den drabbar väldigt olika typer av miljöer. Sårbarheten kan leda till konsekvenser för såväl organisationernas egna IKT-miljöer som de molntjänster som organisationen använder.

Konsekvenserna av sårbarheten begränsar sig inte heller till något visst verksamhetsfält. Sårbarheten kan gälla både kontorssystem, organisationers bakgrundssystem och industrins automationssystem. Sårbarheten är kritisk, eftersom den i praktiken fungerar som en huvudnyckel till den drabbade tjänsten.

”Sårbarheten i Log4j gör en enorm mängd system mottagliga för angrepp. Det är den hittills allvarligaste sårbarheten under det här årtiondet. Log4j kan leda till större konsekvenser än fallet WannaCry år 2017 som globalt orsakade skador i miljardklassen”, konstaterar Juhani Eronen, ledande sakkunnig vid Cybersäkerhetscentret.

Cybersäkerhetscentret informerade om sårbarheten i media, och vi påminde även företagens ledning om att man borde närma sig sårbarheten som en kontinuitetsrisk för organisationens affärsverksamhet. Ett utpressningsprogram kan till exempel helt och hållet hindra organisationen från att utöva sin kärnverksamhet. De verkliga konsekvenserna av sårbarheten kommer att klarna först under de närmaste månaderna, och metoderna för att utnyttja den kommer att stanna i angriparnas verktygslåda i många år framöver.

Typer av skadeprogram Q3/2021



Bland de observationer av skadeprogram som Cybersäkerhetscentrets system Autoreporter samlat in år 2021 urskiljer sig Hummer och FluBot tydligt. Varje månad gjordes omkring 8 500 observationer av Hummer. Flest observationer av enskilda skadeprogram gjordes i juli 2021, då antalet FluBot-observationer var 14 067.

Dataintrång och dataläckage

Under år 2021 inträffade flera dataintrång i världen i samband med vilka brottslingar använde utpressningsprogram mot organisationer. Efter ett dataläckage är det i praktiken omöjligt att få bort informationen från internet.

Typiskt för dataintrången i Microsoft Exchange under våren var att ett så kallat webbskal eller en bakdörr installerades på offrets e-postserver. Förfaringssättet vid dessa dataintrång har varit känt ända sedan år 2020. Utredning kräver mycket teknisk kompetens och mycket resurser, och därför är det bra att ta hjälp av till exempel företag som erbjuder informationssäkerhetstjänster. På våren publicerade vi en guide till stöd för utredningen av dataintrång.

I samband med dataintrång används allt oftare utpressningsprogram

Under det gångna året rapporterades det i Finland och runt om i världen om flera fall där det i efterverkningarna av dataintrånget bland annat förekom att offret hade hindrats från att använda sina egna system och uppgifter med hjälp av ett utpressningsprogram. Mest uppmärksamhet fick fallet Colonial Pipeline i USA som ledde till att en lösensumma betalades.

Enligt organisationens ledning var det inget lätt beslut. Att betala lösen rekommenderas inte, eftersom penningströmmarna upprätthåller brottslingarnas affärsverksamhet och betalande av lösensumman inte innebär att angriparen kommer att överlåta dekrypteringsnyckeln för utpressningsprogrammet till offret.

Behandlingen av dataintrånget mot psykoterapicentret Vastaamo som uppdagats hösten 2020 fortsatte även under år 2021. Vi fick några anmälningar om webbplatser, där personuppgifter för offer för dataintrånget hade publicerats på nytt. När vi fick information om webbplatserna begärde vi att de skulle tas bort. Ett beklagligt faktum är dock att material som en gång blivit offentligt är nästan omöjligt att slutgiltigt få bort från nätet.

Det krävs mycket för att skydda sig mot dataintrång

Dataintrång eller dataläckage kan inträffa i en organisation, trots att man skulle ha gjort allt som står i ens makt för att skydda sina uppgifter. Det kan finnas en tidigare okänd sårbarhet i en tjänst eller på en webbplats, det kan finnas ett fel i en konfiguration, eller så kan en anställds inloggningskoder hamna i händerna på brottslingar.

Det är krävande att skydda sig mot dataintrång. Det är dock möjligt göra det svårt för angriparen att tränga sig in och lättare för den som försvarar sig att upptäcka intrång. Vi vill uppmuntra alla aktörer att även framöver utveckla och allokera resurser för att skydda sig. De resurser som anvisats för detta ändamål kan i många fall vara ganska ringa med tanke på hurdana skador ett cyberangrepp kan orsaka.

”Det är krävande att skydda sig mot dataintrång.

Nätfiske och bedrägerier

Sms-bedrägerier producerades i rekordtakt och på ett mer uppfinningsrikt sätt än någonsin tidigare. Även bedragarnas brottsliga vinning slog alla tidigare rekord.

Finländarna lurades på tiotals miljoner

Även det här året har bedragare erhållit en brottslig vinning på över 30 miljoner euro. Beloppet har stigit med över 60 procent från föregående år. Till polisen rapporteras årligen om tusentals olika typer av bedrägerier i datanätet, och de ekonomiska förlusterna till följd av dem uppgår till tiotals miljoner. Enbart nätfiske efter bankkoder orsakade år 2021 förluster på över åtta miljoner euro, när brottslingar kom över konsumenters bankkoder via webbplatser för nätfiske och tömde bankkonton med hjälp av dem. Polisen tog emot över 800 brottsanmälningar om nätfiske efter bankkoder och till Cybersäkerhetscentret tog emot över 1 800 anmälningar om informationssäkerhetsincidenter.

Nätfiske efter bankkoder har blivit alltmer omsorgsfull och professionell brottslighet. Vanligtvis fiskar man efter användarkoder genom att skicka förfalskade bluffmeddelanden i bankens namn. Brottslingarna har nu upptäckt att bankkoder används även för andra ändamål än bankärenden, vilket kan utnyttjas vid bedrägerier: även i myndighetstjänster loggar användarna in genom att identifiera sig med bankkoder.

”Nätfiske efter bankkoder har blivit alltmer omsorgsfull och professionell brottslighet.

År 2021 lurade bedragare till sig bankkoder med hjälp av meddelanden som hade förfalskats så att de såg ut att komma från en myndighetstjänst, till exempel Mina Kanta-sidor eller Suomi.fi.

I oktober utfärdade Cybersäkerhetscentret en varning, där man varnade för fiske efter bankkoder i olika myndighetstjänsters namn. Varningen fick bra synlighet i media, och det skrevs flera nyhetsartiklar om den. Även i appen 112 Suomi för smarttelefoner som används av uppemot två miljoner finländare informerades om varningen. Den nya kanalen för varningar togs väl emot, och vi hoppas att vi med hjälp av den har kunnat hindra tusentals kunders bankuppgifter från att hamna i händerna på brottslingar.

Även skadeprogrammet FluBot, som spreds explosionsartat bland Android-telefoner i början av året, stjäl bankuppgifter. Dessutom ger det upphov till stora fakturor för offrets telefonabonnemang genom att skicka tusentals sms runt om i världen. Den gula varningen om FluBot som utfärdades i juni togs bort efter att fenomenet lagt sig. Epidemin förnyades dock snart efter att varningen hade tagits bort, varvid varningen aktiverades på nytt i juli. Samma fenomen återvände ännu i förnyad form, och i november publicerades en ny varning om FluBot. Skadeprogrammet skickar bluffmeddelanden som leder till en webbplats där skadeprogrammet laddas ner med förevändningar som snabbt förändras. Traficoms varningar har fått stor synlighet i media.

Sms fick även annars ett starkt fotfäste som ett viktigt redskap för bedrägerier. Det är nästan lika enkelt att förfalska avsändare av sms till telefoner som att förfalska uppgifter om e-postavsändare. Sms har hittills använts för bedrägerier i mindre utsträckning än e-postmeddelanden, så deras trovärdighet anses vara ännu bättre. Därför är det en lockande bedrägerimetod för brottslingar. Från telefonen leder länkar som skickats per sms ändå lika ofta till en webbplats för nätfiske som länkar som skickats per e-post. Vi har fortfarande mycket att göra när det gäller att lära oss att inte klicka på allt.

Föremålens internet och automationssystem

Alla enheter som syns öppet i det offentliga nätet utgör en cybersäkerhetsrisk. Det är enkelt att använda industrins och hushållens IoT-enheter, men enligt vad vi har erfarit tyvärr alltför ofta osäkert. Cybersäkerhetscentret uppmuntrar tillverkarna att utveckla apparater där informationssäkerheten säkerställs på ett bättre sätt och strävar efter att öka deras synlighet. På konsumenternas apparater anger Cybersäkerhetsmärket att tillverkaren har sörjt för apparatens informationssäkerhet på ett lämpligt sätt. För organisationer rekommenderar Cybersäkerhetscentret Cybermätaren.

Riskerna ökar när kontors- och automationssystem integreras

Traditionella kontorssystem (IT) och automationssystem (OT) blir alltmer sammanflätade. Ett bra exempel på detta är Colonial Pipeline som i maj föll offer för ett utpressningsprogram. Det förekom störningar i bränsledistributionen på hela USA:s västkust i flera dagar. Fallet är anmärkningsvärt, eftersom angreppet inte riktades mot distributionsautomationen för bränslen, utan mot affärssystem till stöd för den.

Kritisk produktion kunde inte fortsätta, eftersom penningrörelsen i anslutning till den förhindrades. Till exempel är liknande beroendeförhållanden förknippade med materialflöden inom produktionen och med underhållssystem. Vi uppmanar finländska företag att se över riskerna som är förknippade med tryggandet av produktionen även med tanke på dessa ömsesidiga beroenden.

Det finns fortfarande oskyddade enheter på nätet

I Cybersäkerhetscentrets årliga kartläggning av oskyddade automationsenheter gick vi i genom cirka 12,2 miljoner IP-adresser i den finländska cyberrymden. På nätet hittade vi tyvärr återigen mängder av dåligt skyddade automationsenheter bland företagen och sårbara IoT-enheter bland konsumenterna.

De automationsenheter som företagen använder är traditionellt inte designade för att direkt anslutas till det offentliga nätet och därför är informationssäkerhetskontrollerna av dem inte heller tillräckliga. Om det finns ett behov av att nå en sådan enhet via det offentliga nätet, ska man ta i bruk en tillräckligt säker distansförbindelse.

En enda enhet inom produktionsautomationen som syns i det offentliga nätet försätter hela produktionsnätet i stor fara, eftersom den ger angriparen en möjlighet och en kanal att ta sig in i produktionsnätets övriga delar. Flera tillverkare av konsumentenheter förhåller sig nonchalant till informationssäkerhet. Det ursprungliga sättet att tillverka enheterna kan ha varit sådant att informationssäkerheten inte säkerställts överhuvudtaget, eller så åtgärdar tillverkaren inte alls de sårbarheter som upptäcks. Till exempel som en del av ett botnät som administreras av brottslingar är apparaterna i hemmet ett ständigt hot mot alla tjänster och användare på internet. Botarméer av konsumentenheter kan åstadkomma förödande överbelastningsangrepp.

En angripen IoT-enhet i ditt hem öppnar även hemmet för nätbrottslingar. Konsumenten kan genom sina egna val avsevärt minska denna risk. Det billigaste alternativet har sällan de bästa egenskaperna med tanke på informationssäkerheten. Om det inte går att uppdatera enheten hör den hemma i återvinningen av el- och elektronikskrot.

Cybersäkerhetsmärkets år

Traficoms Cybersäkerhetsmärke hjälper konsumenten att identifiera säkra produkter. Märkets verkningsområde växte i oktober 2021, då Traficom avtalade om ömsesidigt erkännande av Cybersecurity Label med cybersäkerhetsmyndigheten i Singapore. Nu har produkter som fått Cybersäkerhetsmärket därför även godkänts av Singapore.

Därtill utvecklade vi samarbetet genom att ge kommersiella aktörer möjlighet att utföra den tekniska kontrollen i anknytning till beviljandet av Cybersäkerhetsmärket. Den första aktören att utnyttja denna möjlighet var det norska företaget NEMKO, som granskade produkten Smart Hub från Datek. Produkten beviljades Cybersäkerhetsmärket i juni. Vi hoppas att samarbetet med de kommersiella aktörerna kommer att fortsätta vara produktivt även framöver.

Cybervädret 2021 och blicken mot 2022

Riktningen för cybersäkerheten går mot förebyggande åtgärder. Genom reglering strävar man efter funktionssäkerhet och säkerhet, men informationssäkerheten i vardagen kan alla påverka. På fältet utförs ett värdefullt frivilligarbete för att förbättra kännedomen om cybersäkerhet. Vi har bedrivit kampanjer för att informera bland annat äldre om informationssäkerhet.

10 informationssäkerhets-utsikter för 2022

1.

Regleringen omfattar nya teknologier och nya branscher
Inom Europeiska unionen pågår som bäst flera lagstiftningsprojekt som syftar till att bland annat förtydliga spelreglerna för digitala tjänster, skapa artificiell intelligens, göra smarta enheter och datahanteringen säkrare samt precisera olika aktörers skyldigheter ifråga om informationssäkerhet. Genom den nya regleringen skapas och planeras dessutom aktivt nya aktörer inom digital säkerhet för EU:s spelfält.

2.

Teknologin en scen för stormaktskampen
Kampen mellan stormakterna blir allt mer även en kamp om vem som härskar över teknologin i världen. Detta märks i till exempel standardiseringen av teknik där i synnerhet Kina stärker sin roll i enlighet med planen China Standards 2035. Därför är även finländska tekniska innovationer intressanta som föremål för cyberspionage.

3.

Alla hänger inte med i digitaliseringen
Coronapandemin satte fart på digitaliseringen av tjänster, och allt fler tjänster finns tillgängliga på nätet dygnet runt. Digitaliseringen gör det lättare att uträtta ärenden och gör vardagen smidigare – men inte för alla. Brist på digitala färdigheter, en internetanslutning eller språkkunskaper kan försvaga känslan av delaktighet i den digitala miljön. I takt med att tjänster utvecklas är det skäl att ägna ännu mer uppmärksamhet åt tillgänglighet och delaktighet.

4.

Bristen på halvledare fortsätter
Bristen på halvledare visar inga tecken på att lätta. Organisationer kan bli tvungna att vänta på nya apparater i månader och på det sättet vara tvungna att använda apparater som nått slutet på sin livslängd längre. Likaså tar det längre tid än planerat att bygga upp nya skyddslösningar. För butiker som säljer apparater är det värt att vara på sin vakt, eftersom störningarna i tillgången och de stigande priserna lockar även billiga kopior till marknaden. Även om Europa och USA försöker minska sitt beroende av halvledarfabriker i Asien, förväntas bristen fortsätta en bra bit in på år 2022.

5.

Också smarta enheter ska återvinnas
Med hjälp av nya tekniker kan man bidra till att hitta lösningar för att bekämpa klimatförändringen, men en nackdel med den ökande mängden smarta enheter är att även klimatbelastningen ökar. Se alltså till att föra elektroniska och smarta apparater som nått slutet av sin livslängd till återvinningen, reparera apparater om det är möjligt och fråga din försäljare om uppdateringar av dina smarta enheter. Traficoms Cybersäkerhetsmärke är till hjälp när du köper smarta enheter.

6.

Behovet av experter inom cybersäkerhet blir mångsidigare
Ny reglering och det faktum att cybersäkerhet smälter samman med företagens dagliga funktioner ökar allt mer behovet av experter. Företagen söker inte längre renodlade kodare, utan framöver kommer det att finnas en allt större efterfrågan på bredare kompetens inom digitalisering, cybersäkerhet och data.

7.

Gränserna mellan cyberspionage och cyberbrottslighet suddas allt mer ut
Metoderna och verktygen som cyberbrottslingar och -spioner använder sig av påminner allt mer om varandra, och det att cyberbrottsligheten blir mer professionell leder till allt mer avancerade och ekonomiskt motiverade cyberangrepp. Å andra sidan utnyttjar auktoritära stater olika aktörer som mellanhänder för att nå sina mål, vilket gör det svårare att identifiera gärningsmannen och motiven för angreppen.

8.

Inte heller bilarna är skyddade mot cyberangrepp
Nya bilar blir smartare och smartare jämfört med sina föregångare, och i en enda bil kan det finnas flera tiotals olika programvaror. På samma sätt som när det gäller andra programvaror ska man se till att programvarorna i bilen är uppdaterade. Kommer vi att få se det första angreppet med skadeprogram mot bilar under år 2022?

9.

Artificiell intelligens till hjälp vid dataintrång
Artificiell intelligens införs i företagen i allt snabbare takt, och även brottslingarna hänger med i utvecklingen. Med hjälp av artificiell intelligens och maskininlärning kan man göra allt trovärdigare deepfakevideor eller utnyttja bottar för riktat nätfiske. År 2022 kan artificiell intelligens också användas som en del av bedrägerier mot verkställande direktörer, för att hjälpa brottslingar att ta sig in i organisationer.

10.

Användningen av utpressningsprogram i förändring
Även om många organisationer har förstått vikten av säkerhetskopiering och även myndigheterna jagar brottslingarna bakom skadeprogram, är utpressningsprogram inte alls ute ur bilden. Istället för att dölja information kommer man framöver att allt oftare orsaka skada genom dataläckage eller störande av den operativa verksamheten, i synnerhet i OT-nät. Även cyberförsäkringar, som blir allt vanligare globalt, kan bli nya inkomstkällor och incitament för cyberbrottslingar, när lösen betalas ur försäkringsbolagens börsar. Cybersäkerhetscentrets råd kvarstår: betala ingenting till kriminella.

Cybervädret 2021

Varning | Sårbarhet

Januari

Vastaamos **patientuppgifter** delas återigen på nätet

Februari

Bluffmeddelanden med OmaPosti som tema besvärar finländarna dagligen

Mars

Den **kritiska sårbarheten** i e-postservern Exchange utnyttjas aktivt

April

Sårbarheten i applikationen **Pulse Connect Secure** för distansanvändning utnyttjas internationellt vid spionage

Maj

Cybersäkerhetsmärket väcker intresse vid ett internationellt webbinarium om informationssäkerhet i smarta enheter

Juni

Inom **Utvecklingsprogrammet** för cybersäkerheten fastställs åtgärder för att förbättra cybersäkerheten i samhället

Juli

Sårbarheten i **Windows** funktion för bakgrundsutskrift orsakar långvariga bekymmer för organisationer

Augusti

På Instagram sprids en **nätfiskekampanj** som lyckas kapa många användarkonton

September

I komponenten OMI i **molntjänsten Azure** hittas en sårbarhet som gör det möjligt att utföra kommandon med OMI:s tillstånd

Oktober

Vi informerar för första gången om informationssäkerhetsstörningar i appen **112 Suomi**

November

Vi publicerar Finlands första **cybersäkerhetsutredning** om artificiell intelligens

December

Den kritiska **sårbarheten i komponenten Log4j** kräver omedelbara åtgärder för att säkerställa användningen av olika tjänster

Behöver du eller din organisation hjälp med att bekämpa informationssäkerhets-incidenter eller har du frågor om regleringen av cybersäkerheten? Vi utvärderar och godkänner även informationssystem.

Vi utvecklar och övervakar funktionssäkerheten och säkerheten hos kommunikationsnät och -tjänster. Du kan nå oss på följande sätt:

per e-post: kyberturvallisuuskeskus@traficom.fi
kundtjänst: 0295 345 630

Följ oss och våra nyheter
kyberturvallisuuskeskus.fi
@CERTFI
facebook.com/NCSC.FI

Anmäl en informationssäkerhetsincident till oss
kyberturvallisuuskeskus.fi/sv/anmal

Transport- och kommunikationsverket Traficom
Cybersäkerhetscentret

PB 320, 00059 TRAFICOM
tfn 029 534 5000

kyberturvallisuuskeskus.fi

ISBN 978-952-311-777-8
ISSN 2669-8757

TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret