TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

Informations-säkerhetens år 2023

Innehåll

Traficoms publikationer 10/2024
ISSN 2669-8757 (elektronisk publikation)
ISBN 978-952-311-909-3

Inledning

År 2024 har kört i gång raskt, så nu är det bra att stanna upp för en stund och se tillbaka på förra året. Vad hände på cybersäkerhetsfronten? Det hände mycket. När det gäller hot såg vi utpressningsprogram, spridning av bluffmeddelanden samt överbelastningsangrepp. Brottslingarna var opportunistiska och hittade hela tiden på nya metoder att försöka ta sig i organisationers informationssystem eller lura pengar eller personuppgifter av människor. Dessutom fortsatte försöken till cyberspionage aktivt mot organisationer. Det finns inga gränser i den här kriminella verksamheten för hur fräck och omoralisk man kan vara.

Vid Traficom följer vi kontinuerligt fenomen i det digitala samhället och cybersäkerheten. Vi hjälper företag, myndigheter och medborgare att förbereda sig för och identifiera dagens och framtidens cyberhot. Vårt arbete skapar möjligheter för att påverka den tekniska utvecklingen och minimera de utmaningar som den medför.

Olika hot får mycket synlighet i offentligheten och den offentliga diskussionen. Det arbete som kontinuerligt görs inom olika sektorer i samhället för att utveckla cybersäkerheten får ofta mindre uppmärksamhet. Samarbete, informationsutbyte, metoder och teknologier som används i bekämpningen utvecklas hela tiden.

Cybersäkerhet och vardagens informationssäkerhet är små och stora gärningar. Allt utgår från att man är omsorgsfull och alert. Att man ser till att programuppdateringar och informationssäkerheten för enheter och tjänster är i skick. Och dessutom att man hjälper en kompis att till exempel ta i bruk nya smarta enheter.

För organisationer ska informationssäkerhet och att sörja för den utgöra grunden för all affärsverksamhet och operativa verksamhet.
En bra informationssäkerhet och att sörja för den är en central del av samhällsansvaret för organisationer som hör till det moderna digitala samhället.

Dålig informationssäkerhet äventyrar företagets affärsverksamhet och kan i värsta fall innebära att den upphör. Det finns inga genvägar till god informationssäkerhet. Det lönar sig alltså inte att ta genvägar.

Att sörja för informationssäkerheten är att ha ansvar för den egna organisationen, dess anställda, kunder och i slutänden även för cybersäkerheten i hela det finländska samhället.

Det går inte att göra ett cybersäkert Finland på egen hand, utan det förutsätter ett övergripande samarbete mellan alla olika sektorer i samhället. Därför vill jag tacka alla som dagligen arbetar för att främja cybersäkerheten i Finland.

Jarkko Saarimäki
Generaldirektör

> ”En bra informationssäkerhet och att sörja för den är en central del av samhällsansvaret för organisationer som hör till det moderna digitala samhället.

Ps. Du har väl bekantat dig med Cybersäkerhetscentrets **veckoöversikter** och **Cybervädret**? Båda ger viktig och aktuell information om vad som sker inom cybersäkerheten. Ytterligare information Cybersakerhetscentret.fi

Cybersäkerheten utvecklas långsiktigt och strategiskt i Finland

I takt med att samhället digitaliseras är branscher och samhällets olika sektorer alltmer beroende av varandra. I dagens läge är det få störningssituationer som berör endast en bransch eller ett förvaltningsområde. Beredskapen för och svaret på moderna hot förutsätter att samarbetet mellan samhällets olika sektorer är tätt och att informationen förmedlas störningsfritt och snabbt.

Förbindelserna mellan ledning, lägesbild och kommunikation måste fungera. Beslut måste fattas utifrån korrekt information och en korrekt lägesbild. Dagens och framtidens kriser förutsätter även att man satsar alltmer på kommunikation.

Cybersäkerheten är en central del av den övergripande säkerheten i Finland och det finländska samhället. Cybersäkerheten kräver på samma sätt som den övriga säkerheten satsningar och kontinuerlig utveckling för att svara på befintliga och framtida hot. Särskilt nu när det säkerhetspolitiska läget i världen förändras.

Cybersäkerhet går inte att skapa på egen hand och säkerställande av den kräver ett smidigt och förtroendebaserat samarbete mellan företag och myndigheter. I Finland har detta samarbete långa traditioner och har bedrivits på ett täckande och omfattande sätt mellan olika samhällssektorer för att främja cybersäkerheten.

Lagstiftningen, metoderna och standarderna för cybersäkerhet, beredskap och myndighetssamarbete utvecklas hela tiden både i Finland och på EU-nivå. Utbildningen och forskningen i cybersäkerhet stärks kontinuerligt i Finland.

År 2023 förblev hotnivån för cybersäkerheten förhöjd. Traficom och Skyddspolisen i nformerade om hotnivån i april 2023. Senast man meddelade om förhöjd hotnivå var hösten 2022. Orsaken till förändringen är att cyberangrepp blivit allvarligare och mer riktade än tidigare.

Det förekommer allt oftare att en angripare försöker göra intrång i en viss organisation. Dessutom påverkade bedrägerier, överbelastningsangrepp, skadeprogram, utpressningsangrepp mot organisationers IKT-miljöer och nätfiske vardagen för finländarna och organisationer som är verksamma i Finland. **Enligt Cybersäkerhetscentrets bedömning förblir hotnivån förhöjd även 2024.**

Hotnivån mot cybersäkerhet har förblivit förhöjd – antalet riktade angrepp har ökat | Traficom

Cybersäkerhet förutsätter kontinuerligt utvecklingsarbete

I Finland är myndigheternas uppgifter och roller tydliga när det gäller cybersäkerheten. Samarbetet fungerar både på statsrådsnivå och operativ nivå. Man samarbetar operativt varje dag, och myndigheterna har välorganiserade grupper och verksamhetsmodeller för samordning.

Cybersäkerheten och dess utveckling beaktas på många sätt i statsminister Orpos regeringsprogram. Cybersäkerheten syns i högre grad än tidigare i regeringsprogrammet. Finlands cybersäkerhetsstrategi kommer att revideras under regeringsperioden. Beredningen av strategin inleddes 2023. Som ett led i utvecklingsprogrammet för cybersäkerhet (statsrådets principbeslut 2021, Utvecklingsprogram för cybersäkerheten – Valto), som sträcker sig över regeringsperioder, bereddes som tjänsteuppdrag en förvaltningsövergripande utredning om cybersäkerhet ”Utredning om myndigheternas verksamhetsförutsättningar i fråga om cybersäkerhet”. En betydande del av förslagen i utredningen, såsom ökad utbildning i cybersäkerhet, identifiering av kritiska system och säkerställande av deras säkerhet, beaktas i regeringsprogrammet liksom även i större utsträckning i programmet för utveckling av cybersäkerheten 2021.

Ledningsstrukturen för den övergripande säkerheten och cybersäkerheten revideras under regeringsperioden under ledning av statsministern. I reformen säkerställs att ansvarsfördelningen och befogenheterna mellan myndigheterna är tydliga och att informationsutbytet är effektivt samt genomförs de lagstiftningsändringar som dessa förutsätter. Dessutom stärks cybersäkerheten i nära samarbete med företag, näringslivet och tredje sektorn med beaktande av att en stor del av den kritiska infrastrukturen ägs av privata aktörer.

De viktigaste behoven av att utveckla cybersäkerheten inom den närmaste framtiden hänför sig till lagstiftningen. Eftersom verksamhets- och säkerhetsmiljön samt teknologierna förändras snabbt är det viktigt att även lagstiftningen är uppdaterad och hänger med i utvecklingen. För att förbereda sig och bemöta dagens och framtidens cyberhot är det viktigt att det finns välskyddade system och att behöriga myndigheter kan utbyta information allt effektivare och snabbare. Cybersituationer avviker från händelser i den fysiska världen i det att det är avgörande hur snabbt situationerna hanteras – det handlar om minuter och sekunder.

Utöver att utveckla lagstiftningen ska en målinriktad referensram för attribut utvecklas för att främja en trovärdig nationell cybersäkerhet och i ett vidare sammanhang det utrikes- och säkerhetspolitiska inflytandet. När man talar om statlig fientlig cyberverksamhet avses med attribut å ena sidan en analys- och beslutsprocess som gäller identifiering av en ansvarig statlig aktör och å andra sidan ett offentligt tillräknande som gjorts som motåtgärd och som baserar sig på den. En central fråga i bekämpningen av statlig fientlig cyberverksamhet är vem som i sista hand är den statliga aktör som ansvarar för den fientliga cyberverksamheten. Därför förutsätter attributprocessen utöver tekniska uppgifter även omfattande information samt strategisk och utrikes- och säkerhetspolitisk bedömning för att utreda vilken statlig aktör som ligger bakom den fientliga cyberverksamheten och motivet till den samt för att överväga olika reaktionsalternativ.

- Statsrådets principbeslut 2021, Utvecklingsprogram för cybersäkerheten Valto | Statsrådet
- Utredning om myndigheternas verksamhetsförutsättningar i fråga om cybersäkerhet | Statsrådet

Företagen har ett viktigt ansvar i att upprätthålla och utveckla cybersäkerheten

Den helhet som består av cybersäkerhet och -skydd består av flera aktörer. I den har företagen ett viktigt ansvar. De ansvarar för att producera flera viktiga tjänster som är kritiska med tanke på samhällets funktion. Utan den privata sektorns tjänsteleverantörer skulle det i praktiken inte finnas någon elektronisk kommunikation – åtminstone inte tillgänglig för alla medborgare.

Till exempel teleföretagen ansvarar för att alla mobilförbindelser som vi använder fungerar och erbjuder tillträde till exempelvis internet via sina nät. Utan teleföretagen skulle det inte heller finnas någon antenn- eller kabel-tv-distribution eller några antenn- eller kabel-tv-tjänster. Teleföretagen och bankerna erbjuder oss mobilcertifikat och nätbankskoder som vi kan använda för att logga in på e-tjänster och numera uträtta många ärenden hos olika myndigheter.

I Finland ansvarar aktörerna själva för cybersäkerheten inom sektorerna tillsammans med myndigheterna inom sektorerna. I takt med att verksamhetsmiljön förändras behövs allt mer samarbete mellan den offentliga och den privata sektorn. Sådant samarbete, både mellan och inom olika samhällssektorer, har redan långa traditioner inom cybersäkerheten i Finland. Detta samarbete, som även väckt intresse ute i världen, har byggts upp och utvecklats långsiktigt enligt principerna och konceptet för övergripande säkerhet. Under årens lopp har samarbetet intensifierats och verksamhetsmodeller har skapats för det. Därtill överförs de lärdomar som erhållits genom den gemensamma övningsverksamheten fortlöpande i praktiken inom olika sektorer.

Cyberskyddet som helhet bildas tack vare aktörer som omsorgsfullt utför sina uppgifter samt genom samarbete och kontinuerligt informationsutbyte.

> ”Samarbete, både mellan och inom olika samhällssektorer, har redan långa traditioner inom cybersäkerheten i Finland.

Informationssäkerhetens år 2023

Hotnivån förblev förhöjd

Cyberhotnivån, som höjdes 2022, förblev förhöjd under 2023. Finland utsattes aktivt för olika cyberangrepp, bland annat bedrägerier, nätfiskekampanjer och angrepp med utpressningsprogram. Antalet rapporterade fall av incidenter som rapporterades till Cybersäkerhetscentret ökade med cirka 44 procent jämfört med föregående år. Antalet incidenter ökade när det gäller till exempel bedrägerier, försök till dataintrång och bluffmeddelanden. År 2023 publicerade Cybersäkerhetscentret en varning om dataintrång i e-post i M365.

Liksom 2022 var angreppen mer riktade och mer skräddarsydda än under tidigare år. Olika cyberhotsaktörers skicklighet har utvecklats bland annat genom lättillgängliga tjänster och automatisering. Hotaktörer med olika motiv utnyttjar samma skadliga program och kritiska sårbarheter. Bland annat på grund av detta är det allt svårare att urskilja aktörerna på basis av verksamheten.

Rysslands fortsatta anfall mot Ukraina har synts i cybermiljön till exempel i form av överbelastningsangrepp i Europa av proryska hacktivister mot åtgärder som anses vara rysslandsfientliga. I Finland observerades överbelastningsangrepp särskilt från början av hösten. I offentligheten uppgavs till exempel att politiska orsaker var motiven till angreppen. Motsvarande verksamhet var vanlig också på andra håll i Europa. Överbelastningsangrepp mot finländska organisationer hade inga betydande konsekvenser.

I synnerhet nationellt samarbete med låg tröskel mellan myndigheter och företagsfältet är viktigt för att begränsa konsekvenserna.

I flera av incidenterna blev det tydligt att aktiva åtgärder av organisationen var avgörande för att begränsa konsekvenserna av angreppen. På basis av en analys synliggjorde observationerna av incidenter under 2023 till exempel betydelsen av att införa flerfaktorsautentisering i organisationerna.

Mellersta Nylands samkommun för utbildning Keuda fick 2023 erkännandet Vägvisare för informationssäkerheten för sin öppna kommunikation och sitt agerande när samkommunen utsattes för ett angrepp med utpressningsprogram. Öppen och snabb kommunikation vid angrepp med utpressningsprogram hjälper organisationen att utreda och återhämta sig från situationen samt stöder även andra aktörer i beredskapen mot cyberhot.

Vägvisare för informationssäkerheten | Cybersäkerhetscentret

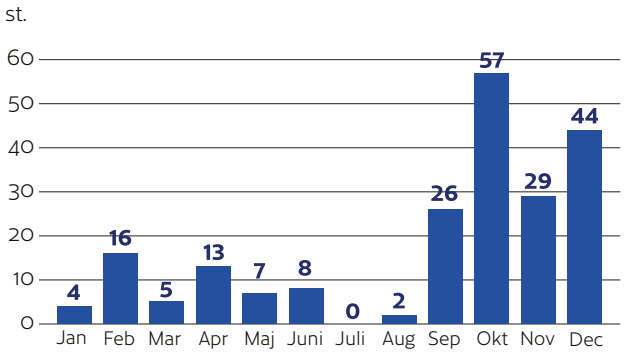
Överbelastningsangrepp

Vid överbelastningsangrepp styrs en stor mängd trafik till webbplatser eller -tjänster. För användaren syns detta på så sätt att webbplatserna inte kan nås eller fungerar mycket långsamt. Överbelastningsangrepp är enkla att utföra och har en effektfull angreppsteknik. De får också ofta uppmärksamhet i medier. I de flesta fall har överbelastningsangrepp inga synliga effekter för användarna, och även i värsta fall leder de främst till korta dataavbrott i offentliga webbtjänster.

I dagens läge är överbelastningsangrepp särskilt vanliga som en form av hacktivism. Hacktivism är cyberbrottslighet där motiven är politiska i stället för ekonomiska fördelar. Genom överbelastningsangrepp visar man missnöje med ett politiskt beslut eller annan verksamhet som bedrivs av det angripna målet och försöker påverka informationsmiljön runt fallet. Dessutom kan även korta dataavbrott öka misstron bland den angripna aktörens kunder och intressenter. Hacktivismen har ökat i synnerhet efter att Ryssland inledde den aktiva fasen av angreppskriget i Ukraina år 2022. Både pro-ryska och pro-ukrainska hacktivistgrupper har använt sig av överbelastningsangrepp som en metod för informationspåverkan.

I hemlandet rapporterades överbelastningsangrepp särskilt på våren den 4 april när Finland anslöt sig till Nato och under hela hösten. I synnerhet den pro-ryska hacktivistgruppen NoName057(16) riktade överbelastningsangrepp mot inhemska organisationer i olika sektorer 2023. NoName brukar hylla överbelastningsangreppen på sin Telegram-kanal, även om angreppet inte hade några konsekvenser för målwebbplatsens funktion. En del överbelastningsangrepp som påverkade funktionen för den offentliga förvaltningens och statsförvaltningens webbplatser noterades även i de inhemska medierna. Organisationer berättade offentligt att de blivit utsatta för överbelastningsangrepp om webbplatserna var ur bruk på grund av det. År 2024 anses överbelastningsangrepp inte längre medföra skada på organisationens anseende. Vilken organisation som helst kan bli föremål för överbelastningsangrepp och organisationerna bör också förbereda sig på överbelastningsangrepp på applikationsnivå.

Anmälningar av överbelastningsangrepp som Cybersäkerhetscentret behandlat 2023



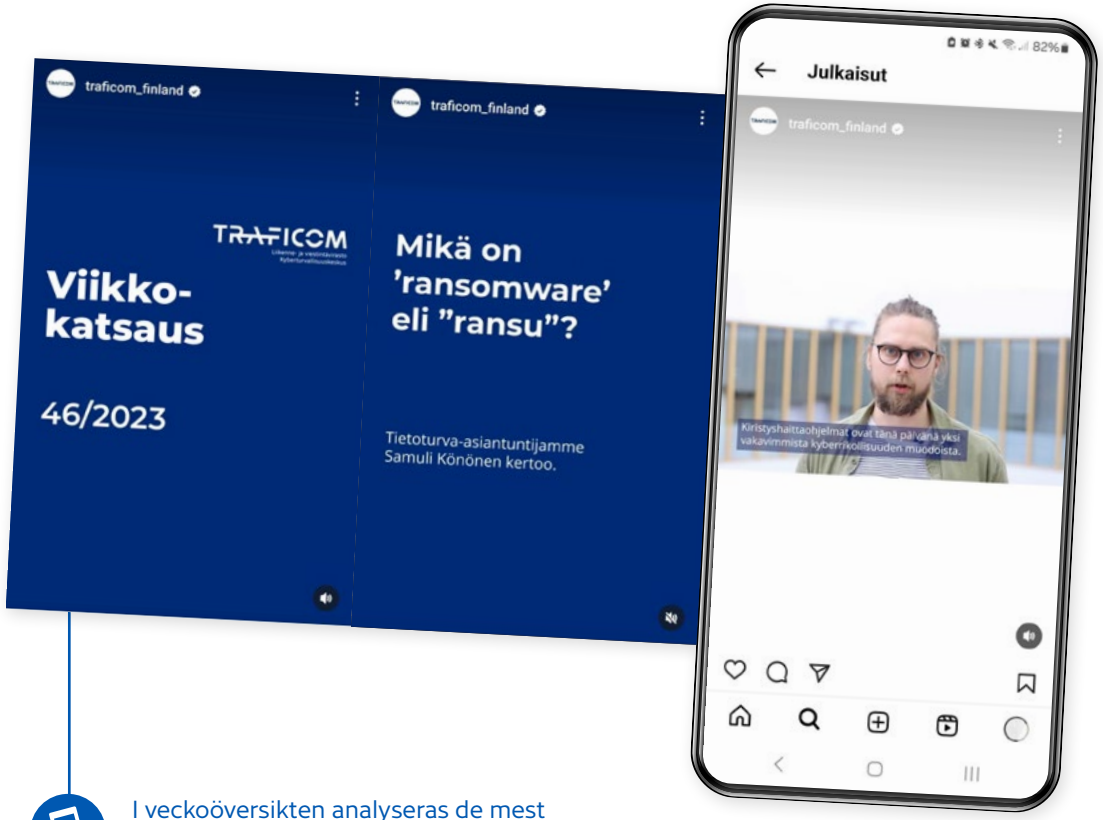
> ”I dagens läge är överbelastningsangrepp särskilt vanliga som en form av hacktivism.

Utpressningsprogram

Fallen av utpressningsprogram ökade tydligt i Finland under slutet av året, då fler fall rapporterades än under tidigare kvartal. Fallen har berört flera branscher, men det har varit möjligt att begränsa deras effekter med organisationernas åtgärder. Till exempel uppdaterade säkerhetskopior har räddat situationen i många organisationer.

För aktörer som sysslar med utpressningsprogram kunde man 2023 generellt notera att de har utvecklats och blivit alltmer verkningsfulla och professionella. Allvarliga fall av utpressningsprogram har ute i världen rapporterats till exempel inom statsförvaltningar, rättsväsendet och hälsovårdssektorn. I dessa fall har det till exempel läckt känsliga personuppgifter och återhämtningen kan ha tagit från flera veckor upp till månader. Det vanligaste utpressningsprogrammet i Finland 2023 var Akira, som i synnerhet rapporterades i slutet av året.

Angrepp med utpressningsprogram orsakar i allmänhet betydande besvär och kostnader för organisationer. Det är ofta svårt att reagera på utpressningsprogram efter att ett angrepp har börjat. Bra beredskap ger mycket bättre utgångspunkter att agera när en incident inträffar.



I veckoöversikten analyseras de mest betydande nationella och internationella cyberhändelserna varje vecka

Läs mer om våra produkter för lägesbilder på sidan 16.

Nätfiske och nätbedrägerier

I fråga om nätfiske och nätbedrägerier gjordes antalsmässigt flest anmälningar om nätfiske av bankkoder. Man försökte komma åt bankkoder genom att använda olika sektorers namn såsom banker, skattemyndigheten, polisen, FPA och andra myndigheter och företag i ett mycket brett spektrum. Det näst livligaste bedrägeriet var nätfiske av Microsoft M365-användarnamn som Cybersäkerhetscentret publicerade en allvarlig varning om vecka 42. Med användarnamn som man fått genom nätfiske gjordes hundratals dataintrång i e-postkonton, men som tur var minskade antalet efter att varningen publicerats.

I offentligheten rapporterades rikligt med informations- och cybersäkerhetsproblem runt om i världen som grundade sig på olika lösningar med artificiell intelligens, till exempel i anslutning till säkerheten vid val. Observationer av cyberincidenter på finska som grundar sig på artificiell intelligens var ännu sällsynta i Finland 2023. Cybersäkerhetscentret fick kännedom om en högklassigt genomförd djupförfalskning (deepfake) baserad på artificiell intelligens där man klonat rösten hos en organisations vd och begärde en stor penningöverföring, men inte heller i det fallet användes finska.

Sommaren 2023 publicerade vi en informationssäkerhetskampanj i sociala medier med målet att öka medvetenheten om bedrägerier och nätfiske på ett lättsamt sätt.

Läs mer om Cybersäkerhetscentrets kampanjer på sidan 19

Man har tagit itu med förhindrande av bluffsamtal genom intensivt samarbete mellan myndigheter och teleföretag redan under flera år. Genom en föreskrift av Traficom som trädde i kraft i början av oktober 2023 ålades teleoperatörer att ännu bättre avvärja utländska samtal som maskerats som finländska, även i fråga om mobilnummer. Alla finländska teleföretag som tar emot trafik från utlandet använder nu filtrering av samtal. Vid Traficom bereds för tillfället en föreskrift som syftar till att i framtiden bekämpa även sms-bedrägerier.

Det arbete som har gjorts i Finland för att förhindra bluffsamtal har även väckt exceptionellt aktivt internationellt intresse, eftersom den modell som tagits i bruk är mycket avancerad även i internationell jämförelse. Den lösningsmodell som tagits i bruk presenterades av finländska myndigheter och teleföretag bland annat i Förenta staterna våren 2023.

Spärr av förfalskade telefonnummer | Youtube (på finska)

Sårbarheter

År 2023 var livligt när det gäller sårbarheter. Över 20 000 unika sårbarheter enligt CVE-sårbarhetsidentifikationen publicerades i världen. Vissa av sårbarheterna är mer kritiska än andra. Av dessa framträder i synnerhet sårbarheter som möjliggör utnyttjande på distans i Cybersäkerhetscentrets vardag. En kritisk sårbarhet kan ge en angripare möjlighet förutom till dataintrång även att installera ett utpressningsprogram. Cybersäkerhetscentret publicerar årligen cirka 30–40 sårbarhetsmeddelanden om de mest kritiska sårbarheterna som gäller användare i hemlandet.

Cybersäkerhetscentret följer dagligen nyheter och diskussioner om sårbarheter. I de allvarligaste fallen kartlägger Cybersäkerhetscentret inhemska användare och kontaktar direkt organisationerna om det finns misstankar om eller observationer av en sårbar produkt. Utrustning som är sårbar över nätet är ett lätt mål för angriparna. År 2023 användes till exempel en sårbarhet hos nätverksutrustningstillverkaren Cisco som språngbräda i flera av fallen av utpressningsprogram i Finland. Enligt ett känt informationssäkerhetsföretag är i synnerhet kritiska sårbarheter viktiga för aktörer som använder sig av utpressningsprogram. Till exempel aktörsgruppen Lockbit utnyttjade sårbarheten Citrix Bleed i sina angrepp 2023 som orsakade globala konsekvenser.

Utnyttjandet av sårbarheter sker snabbare år för år. Efter att en kritisk sårbarhet publicerats kan man redan under de närmaste dagarna observera aktivitet av angripare runt om i världen. Lyckligtvis är informationsutbytet aktivt i cybervärlden och information om utnyttjade sårbarheter sprids. I sin kommunikation om och kartläggning av sårbarheter i Finlands nät prioriterar Cybersäkerhetscentret sårbarheter som redan utnyttjats i världen. En kritisk redan utnyttjad sårbarhet som ger en angripare möjlighet att utföra kommandon på distans i en nättjänst eller nätverksenhet är ofta det mest kritiska exemplet på årsnivå. Lyckligtvis förekommer det på årsnivå bara några sådana här sårbarheter i lösningar som också är populära i Finland som kräver aktivare åtgärder och arbetstimmar av såväl myndigheter som aktörer inom den privata sektorn.

Vi informerar om aktuella informationssäkerhetsfenomen i flera kanaler. Du hittar information om sårbarheter i utrustningar och korrigerande uppdateringar på till exempel Instagram.

Cyberspionage

I likhet med året innan fortsatte försöken till cyberspionage aktivt under 2023. Man strävade ideligen efter att hitta olika sårbarheter eller svagt skyddade användarnamn i tjänster som finländska organisationer använder.

Riktade skadliga e-postmeddelanden och skadeprogram i mobiltelefoner utnyttjades som en del av cyberspionage. Dessutom var molntjänster som användes i stor omfattning utsatta för cyberspionage. En del av verksamheten tyder på verksamhet av statliga aktörer utifrån myndighetskällor samt offentliga, kommersiella eller andra källor.

Ett internationellt fenomen var att sårbarheter i nätverksenheter och e-postsystem utnyttjades i allt större omfattning vid cyberspionage. Sårbara routrar i hem och småföretag samt servrar för webbaserade databaser utnyttjades i stor utsträckning i statliga aktörers verksamhetsmiljöer i syfte att komma närmare det önskade objektet och utplåna den ursprungliga trafikkällan.

Rysslands anfall mot Ukraina syntes fortfarande i cyberspionage och -påverkan. I Ukraina observerades under året till exempel flera störande angrepp mot kritiska system, e-postkampanjer med nätfiske efter information och kampanjer för att sprida skadliga program.

Cyberspionage kan öka direkt eller indirekt i och med Finlands medlemskap i Nato. På andra håll i Europa har cyberspionage riktats mot till exempel aktörer, logistik, produktutveckling inom industrin och teknologisektorn i anslutning till krig.

Kommunikationsnäten fungerade stabilt i Finland 2023

År 2023 fungerade kommunikationsnäten stabilt i Finland. Det förekom klart fler avbrott i tjänster än under det föregående året, men däremot minskade antalet allvarliga avbrott. Vid enstaka avbrott uppstod tillfälliga störningar i regionala tjänster eller i nödtrafiken, men avbrotten var i huvudsak kortvariga. Väderförhållandena var betydligt stormigare än föregående år, vilket bidrog till att antalet störningar orsakade av elavbrott fördubblades jämfört med 2022. Vid en granskning på lång sikt fortsätter antalet funktionsstörningar i allmänna kommunikationstjänster och i synnerhet antalet allvarliga felsituationer att minska, fastän antalet betydande funktionsstörningar totalt ökade avsevärt i jämförelse med det statistiskt exceptionella fjolåret.

Myndigheterna har ett nära samarbete med de finländska teleföretagen för att trygga nätens funktion.

Skada på undervattensinfrastrukturen i oktober 2023

Den kanske mest framstående cybersäkerhetsincidenten 2023 var skadan på undervattensinfrastrukturen i Finska viken i oktober 2023: På efternatten den 8 oktober observerades ett läckage och en störning på grund av det i gasledningen Balticconnector mellan Finland och Estland. Söndagen den 8 oktober Cybersäkerhetscentret vid Transport- och kommunikationsverket fick information av ett finländskt teleföretag om att sjökabeln mellan Estland och Finland gått av i Finska viken, och samma veckoslut skadades även ett annat teleföretags sjökabel mellan Sverige och Estland så att den förmedlade trafik med lägre kapacitet än normalt.

Sörjandet för driftssäkerheten och beredskapen för de allmänna kommunikationsnäten och -tjänsterna (det vill säga televerksamheten) har ända sedan 1990-talet varit en del av den lagstiftning samt den myndighetsstyrning och -övervakning som gäller aktörerna. Detta och Cybersäkerhetscentrets kontinuerliga samarbete med teleföretagen har en stor betydelse för att bland annat avbrutna sjökablar knappt har några synliga konsekvenser alls för teleföretagens kunder.

Också i fallet i oktober överförde teleföretaget enligt normal beredskapspraxis kabeltrafiken mellan Finland och Estland direkt till en reservförbindelse och telekommunikationen mellan Finland och Estland fungerade således problemfritt. Avbrottet påverkade alltså inte de finländska eller estländska kommunikationstjänsternas funktion.

Cybersäkerhetscentret skapade en lägesbild över fallet. Centret följde hur reparationerna av kabeln framskred i nära samarbete med teleföretaget och andra myndigheter, såväl nationellt som internationellt. Genom denna verksamhet stödde man statsrådets beslutfattande.

I Finland och Estland fortsätter förundersökningsmyndigheterna att behandla fallet i oktober. Cybersäkerhetscentret fortsätter det nationella och internationella samarbetet med teleföretag och andra myndigheter för att skydda infrastrukturen för kommunikationsnät samt förebygga, upptäcka och avhjälpa eventuella problem.

Året 2023 för Cybersäkerhetscentret vid Traficom

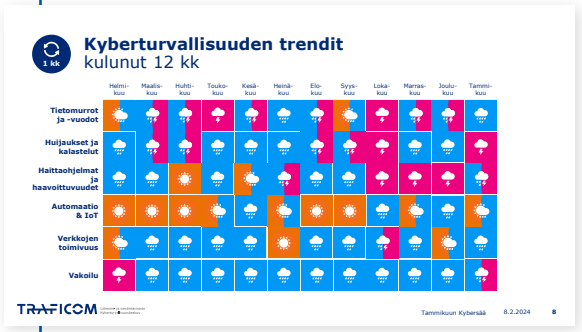
Transport- och kommunikationsverkets och i synnerhet Cybersäkerhetscentrets betydelse som en säkerhetsmyndighet för hela samhället har ökat i en omvärld med förändrad säkerhet under de senaste åren. Cybersäkerhetscentret kan med hjälp av observationsförmåga och informationsutbyte i nätverk tillsammans med sina partner snabbt svara på cyberhot som påverkar samhället och avsevärt minska hotens konsekvenser för samhället, den digitala infrastrukturen och medborgarna. Cybersäkerhetscentret bedömer att enbart dess hantering av informationssäkerhetsincidenter och åtgärder för att hjälpa medborgarna varje år ger samhället en stor nettonytta i euro.

Stöd för lägesuppfattningen av cybersäkerheten i samhället

Cybersäkerhetscentrets uppgifter omfattar att ta fram en kombinerad lägesbild över den nationella cybersäkerheten. Centret samlar in information om datanätshändelser och förmedlar den till olika aktörer. Vid skapandet av lägesbilden utnyttjas nationella och internationella källor i stor omfattning, såsom nätverk för försörjningsberedskapskritiska organisationer, andra säkerhetsmyndigheter samt Cybersäkerhetscentrets officiella nationella och internationella samarbetsnätverk, som grundar sig på frivillighet och ömsesidigt förtroende. Cybersäkerhetscentret får dessutom årligen över tiotusen frivilliga anmälningar av till exempel medborgare. Cybersäkerhetscentrets kunder utnyttjar informationen om lägesbilden för att utveckla sin beredskap och i sin dagliga verksamhet.

Ett exempel på en av centrets offentliga lägesbildsprodukter kan nämnas sammandraget över lägesbilden som utkommer varje vecka i Cybersäkerhetscentrets veckoöversikt, där man analyserar de mest betydande nationella och internationella cyberhändelserna under respektive vecka. I Cybervädret som utkommer månatligen granskar man i sin tur utvecklingsförlopp som påverkar cybersäkerheten på längre sikt. Både Veckoöversikten och Cybervädret finns tillgängliga på Cybersäkerhetscentrets webbplats. Cybersäkerhetscentret producerar också en strategisk lägesbild över cybersäkerheten för den högsta statsledningens bruk.

Cybersäkerhetscentrets veckoöversikt | Cybersäkerhetscentret



Målet med cybervädret är att berätta om händelser i cybervärlden så begripligt och koncist som möjligt.

Cyberväder – aktuellt om informationssäkerhet | Cybersäkerhetscentret

Cybersäkerhetscentrets lägesbildsprodukter har en viktig roll när det gäller att utveckla den samhälleliga lägesförståelsen av cybersäkerheten, dess verkningsfullhet och beredskap. Det gjordes en enkät om centrets offentliga lägesbildsprodukter under 2023 och de som svarade på enkäten gav produkterna vitsordet utmärkt (medeltalet var 4,3 på skalan 0–5).

Det internationella samarbetet intensifierades under 2023

Cybersäkerhetscentret har dagligen tätt samarbete med inhemska och utländska partner och nätverk. Detta inbegriper till exempel förmedling av information om och lägesbilden över av cybersäkerheten samt möten, utbildningar och övningar. I och med det internationella samarbetet ökar kompetensen och medvetenheten om det rådande läget beträffande cyberhot. Samarbetet bidrar således till att förebygga cyberhot mot Finland.

Internationella nätverk och internationellt samarbete har också en viktig roll i utredningen av olika akuta informationssäkerhets- och cyberincidenter. Även skalning av läget beträffande cyberhoten i Finland till ett internationellt läge är möjlig genom nätverken.

Under 2023 fortsatte de sakkunniga vid Cybersäkerhetscentret att intensifiera de bilaterala relationerna till centrala partnerländer, såsom Sverige och Estland. Påverkan och samordning av centrets internationella frågor stärktes även genom en ny befattningsbeskrivning för chefen för internationella ärenden.

Centrala teman i det internationella cybersäkerhetssamarbetet 2023 var operativt samarbete, utveckling av samarbetet på strategisk nivå inom EU och ett flertal lagstiftningsprojekt som gäller cybersäkerhet, också på EU-nivå. Vid sidan av EU-helheterna fortsatte Cybersäkerhetscentret de nationella åtgärderna som en del av den nationella Nato-samordningen. I och med medlemskapet i Nato utökades det internationella samarbetet till nya områden. Övningsverksamheten fortsatte att vara aktiv. En lyckad verksamhet i olika säkerhetssituationer förutsätter utöver uppdaterade planer även regelbunden övning.

Det finns information på webbplatsen för Cybersäkerhetscentret vid Traficom om övningar som gäller cybersäkerhet

Övningar | Cybersäkerhetscentret

Övningsverksamheten fortsatte att vara aktiv

En lyckad verksamhet i olika säkerhetssituationer förutsätter utöver uppdaterade planer även regelbunden övning. Övningar ger värdefull information för utveckling av organisationers operativa verksamhet, ledning, kommunikation och lägesbildsverksamhet.

Under 2023 fortsatte övningar som gäller cybersäkerhet aktivt både i hemlandet och utomlands. I hemlandet deltog centrala tjänsteleverantörer mer i övningarna än under tidigare år. I övningarna betonades granskningen av ansvarsområden för operativa gränssnitt och avtalen som hänför sig till dem. En cyberhot kan också rikta sig mot en tjänstepartner och därigenom yttra sig i den egna verksamheten.

I framtiden kommer man särskilt vid stora nationella övningar i större utsträckning att granska sektorernas interna leveranskedjor och beroendet mellan sektorerna.

Prognostiseringsarbete stöder beredskap för framtidens fenomen

Framtids- och prognostiseringsarbete utvecklades för att ha beredskap för framtida fenomen och den tekniska utvecklingen samt för att stärka det förutseende tänkandet i hela centret. Dessutom fortsatte man att skapa ett samarbete med olika sektorer i samhället.

Fokus på framtids- och prognostiseringsarbetet 2023 var att granska hur olika cyberscenarier förverkligas för att förstå eventuella utvecklingsförlopp i den framtida verksamhetsmiljön. I prognostiseringsarbetet fortsatte man att bedöma effekterna av artificiell intelligens, och Traficom började utarbeta en tredje utredning om artificiell intelligens. I utredningen, som publiceras under vintern 2024, behandlas utnyttjande av artificiell intelligens för att främja cybersäkerhet och cybersäkerhetslösningar som baserar sig på artificiell intelligens. Utredningen är den tredje inom detta tema och kompletterar tidigare utredningar om artificiell intelligens som handlade om riskhantering och cyberangrepp som artificiell intelligens möjliggjort. I utredningarna har man hört en stor grupp experter i informationssäkerhetsbranschen inom privata och offentliga sektorn samt vid forskningsinstitut. Utredningarna har genomförts i samarbete med Försörjningsberedskapscentralen.

I prognostiseringsarbetet behandlades dessutom cybersäkerhet och riskhantering i lokala mobilnät. Aktörer som är kritiska för många av samhällets funktioner kommer sannolikt att framöver utnyttja lokala mobilnät som är skräddarsydda för deras behov för att digitalisera och effektivisera sin verksamhet. Dessa nätlösningar är förknippade med nya typer av risker och kompetenskrav, som det är viktigt att beakta när näten förverkligas. Även publikationer om ovanstående teman producerades för Cybersäkerhetscentrets webbplats. Utredningarna och anvisningarna genomfördes i samarbete med Försörjningsberedskapscentralen.

Traficom ordnar det tredje 5G-hackathonet 2024. Evenemanget Hack the Networks ordnas i maj, och i årets hackathon ligger fokus på säkerheten i lokala 5G-nät som används i kritisk infrastruktur. Läs mer på hackthenetworks.fi (på finska)

- Cyberangrepp som möjliggörs av artificiell intelligens | Traficom (på finska)
- Cybersäkerhet och riskhantering vid tillämpning av artificiell intelligens | Traficom (på finska)
- Anvisning om cybersäkerhet och riskhantering i lokala mobilnät | Cybersäkerhetscentret (på finska)

Den andra delen av utredningen av Cybersäkerhetscentret vid Traficom och Försörjningsberedskapscentralen om cyberattacker som möjliggörs av artificiell intelligens presenterades i slutet av 2023.

Ökad medvetenhet samt kommunikation

Kommunikationen har en central roll i beredskapen för och avvärjandet av cyberhot. När samhället digitaliseras i snabb takt är det viktigt med kompetens i informationssäkerhet och att den hela tiden utvecklas. Utan kännedom om olika hot kan man inte ha beredskap för eller avvärja dem.

Frågor om cybersäkerhet och hot i synnerhet lyfts mycket snabbt fram i den offentliga debatten. De intresserar och väcker även oro. När man diskuterar cybersäkerhet är det viktigt att diskussionen förs utifrån korrekt och aktuell information. Traficom svarar på detta informationsbehov genom att ständigt producera och dela information om cybersäkerhet till olika målgrupper. Som stöd för den högsta statsledningens beslutsfattande om cybersäkerheten produceras en strategisk lägesbildsanalys. Cybersäkerhetscentrets veckoöversikt som publiceras varje vecka och cyberväder som publiceras varje månad berättar för allmänheten om till exempel hurdana bluffmeddelanden eller nätfiskekampanjer de kan råka ut för i sin vardag.

Seminariet Informationssäkerhet, som årligen ordnas i samarbete med Försörjningsberedskapscentralen, samlade över 2 000 deltagare i oktober förra året. Via Traficoms webbplats och sociala mediekonton når man dagligen många olika målgrupper. Dessutom ger de sakkunniga vid centret regelbundet intervjuer till medier. På webbplatsen tillhandahålls anvisningar och handböcker samt tips för att utveckla de vardagliga kunskaperna i informationssäkerhet. Mässor och evenemang samt informationskampanjer till olika målgrupper är en del av metoderna som syftar till att öka kunskapen om cybersäkerhet i samhället.

År 2023 påbörjades planeringen och skapandet av ett koncept för en storriksomfattande informationskampanj om cybersäkerhet för allmänheten. Kampanjen genomförs i samarbete med Myndigheten för digitalisering och befolkningsdata samt Centralkriminalpolisen i slutet av våren 2024.

Digikaistas informationssäkerhetskampanj nådde effektivt målgruppen i Meta till ett förmånligt CPM-pris.

Läs mer om medborgarnas informationssäkerhetskunskaper på sidan 29.

Nätverkssamarbetet utvecklades ytterligare under 2023

Cybersäkerhetscentrets nätverkssamarbete utvecklades kraftigt 2023. Betydelsen av ISAC-informationsutbytesgrupper (Information Sharing and Analysis Centre) var stor i synnerhet när det gäller att skapa en lägesbild samt i det ömsesidiga informationsutbytet mellan samhällets kritiska sektorer i fråga om beredskap och störningssituationer.

Intresset för nätverksverksamhet ökade under det senaste året. Flera nya organisationer anslöt sig till ISAC-informationsutbytesgrupperna, och välfärdsområdena bjöds in till informationsutbytesgruppen för social- och hälsovårdssektorn. Under året grundades nya ISAC-informationsutbytesgrupper för kommunsektorn, informationssäkerhetsföretag och aktörer inom energisektorn. Samma utveckling fortsätter även 2024, eftersom man i år har planerat att grunda informationsutbytesgrupper bland annat för aktörer inom fastighets- och byggsektorn samt inom högteknologi.

Informationsutbytet i anslutning till nätverken internationaliserades under 2023. Finland har varit en aktivare medlem än tidigare i internationella forum och även bilateralt bildande av nätverk på internationell nivå har effektiverats avsevärt.

Även samarbetet och informationsutbytet mellan myndigheter utvecklades aktivt. Den så kallade NIS-samarbetsgruppen mellan tillsynsmyndigheterna beredde sig på verkställande av det nationella NIS2-direktivet.

NIS2-direktivet bland annat ökar antalet sektorer som ska övervakas och medför ytterligare uppgifter för befintliga tillsynsmyndigheter. Under 2024 utökas NIS-samarbetsgruppen avsevärt när nya myndigheter som övervakar NIS2-direktivet ansluter sig. Under 2023 utökade Traficom i föregripande syfte sin befintliga rådgivningstjänst för informationssäkerhet för tillsynsmyndigheterna. Dessutom har informationsutbytet mellan säkerhetsmyndigheter redan från tidigare varit aktivt och fortsätter att vara det på grund av förändringen i säkerhetsmiljön.

Den samhälleliga betydelsen av informationsutbytesgrupper som fungerar som förtroendenätverk har ökat under det gångna året, och nätverken utgör en allt viktigare del av den nationella lägesbilden över cybersäkerheten och hanteringen av störningssituationer. Under 2023 effektiviserades förtroendenätverkens informationsutbyte, och även informationsutbytet över sektorsgränserna förbättrades.

I informationsutbytesgrupperna behandlades beredskap och hybridpåverkan mer än tidigare. Dessutom har man satsat mer än tidigare på cyberövningar.

Cybersäkerhetscentret satsade även på att förmedla uppdaterad information till olika nätverk. Exempel på detta är en sektorrapport varje vecka som pilottestats under hösten samt operativa informationsutjämningar som ordnas med kort varsel vid allvarliga och akuta informationssäkerhetshot. En del av informationsutjämningarna har ordnats förutom för förtroendenätverken, även för aktörer som är kritiska för försörjningsberedskapen. Man fick över sexhundra deltagare med en dags varsel till en informationsutjämning som handlade om betydande informationssäkerhetshot.

> ”Under året grundades nya ISAC-informationsutbytesgrupper för kommunsektorn, informationssäkerhetsföretag och energisektorn.

Samhällets säkerhet främjades genom projekt för utveckling av cybersäkerheten

Cybersäkerhetscentret har under de senaste åren genomfört flera projekt för att förbättra cybersäkerheten för aktörer som är livsviktiga för samhället och genom det hela samhällets beredskap och cybersäkerhet. I dessa projekt har Försörjningsberedskapscentralen haft en central roll i form av att både finansiera projekten och fungera som stöd vid genomförandet av dem. Även finansministeriet har deltagit i finansieringen av Cybersäkerhetscentrets utvecklingsprojekt.

Föremålet för de utvecklingsprojekt som Försörjningsberedskapscentralen finansierar och stöder är företag som är livsviktiga för samhället och deras cybersäkerhet. Målet för de utvecklingsprojekt som finansministeriet finansierar och stöder är å sin sida utveckling av cybersäkerheten inom den offentliga förvaltningen.

Genomförda tjänster är till exempel

- **Havaro**,som upptäcker allvarliga informationssäkerhetshot mot finländska företag och varnar om dem. Havaro.fi/sv
- **Hyöky**, nationell kartläggning av angreppsytan för att förbättra cybersäkerheten i kommunerna. Hyöky | Cybersäkerhetscentret
- **Cybermätaren**, en gratis utvärderings- och utvecklingstjänst för cybersäkerhet. Den är ett konkret verktyg för organisationers ledning och informationssäkerhetsexperter för hantering av cybersäkerheten, sektorspecifik jämförelse och styrning av utvecklingssatsningar. Kybermittari.fi

De utvecklingsprojekt som finansieras av Försörjningsberedskapscentralen finansieras ur centralens program Digital säkerhet 2030 och följer de mål som ställts upp i programmet.

Utvecklingsprojekt som finansieras av finansministeriet har finansierats ur programmet Genomförandeplan för digital säkerhet inom den offentliga förvaltningen 2020–2023 (Haukka).

Stöd för utveckling av företagens informationssäkerhet

År 2023 beviljade Cybersäkerhetscentret 251 företag sammanlagt cirka 5,2 miljoner euro i stöd för utveckling av informationssäkerheten för att förbättra företagens egen informationssäkerhet. Stöd på högst 15 000 euro har beviljats till ett belopp av 3,2 miljoner euro och stöd på högst 100 000 euro har beviljats till ett belopp av 2 miljoner euro. Under året behandlade Cybersäkerhetscentret stödansökningar från 409 företag.

Cirka 40 procent av stödansökningarna avslogs bland annat på grund av att företaget inte uppfyllde de lagstadgade kraven för beviljande av stödet eller att stödansökan var bristfällig, varvid man inte kunde försäkra sig om att kraven för beviljande av stöd uppfylldes. Före slutet av året hade totalt 740 företag ansökt om cirka 19 miljoner euro i stöd, emedan det endast hade reserverats 6 miljoner euro för beviljande av stöden. Den resterande delen på 0,8 miljoner euro av det reserverade anslaget på 6 miljoner euro beviljas i början av 2024.

Erfarenheter av Cybersäkerhetsmärket utnyttjas aktivt i uppföljning och påverkande av EU:s cybersäkerhetskra

Cybersäkerhetsmärket, som offentliggjordes av Cybersäkerhetscentret 2019, visar att en produkt eller tjänst som är försedd med märket uppfyller Traficoms krav på en god basnivå för informationssäkerheten. Kraven för märket baserar sig på en europeisk standard. Märket kan beviljas smarta enheter som kan anslutas till internet och som är avsedda för konsumenter, det vill säga så kallade IoT-enheter. Sådana enheter är till exempel smarta tv-apparater, smartarmband och hemmaroutrar.

Under 2023 beviljades en ny enhet Cybersäkerhetsmärket. För närvarande är märket i kraft för 25 enheter. Samarbetet med cybersäkerhetsmyndigheten i Singapore som inleddes 2021 bidrog till ökningen av antalet märken.

Cybersäkerhetsmärkets roll i fråga om att visa produkters informationssäkerhet kommer att minska under de kommande åren i och med de ändringar av EU-reglering som kommer att träda i kraft. Information som produceras genom verksamheten för Cybersäkerhetsmärket utnyttjas aktivt i uppföljningen av och påverkandet av EU:s cybersäkerhetskrav. Cybersäkerhetscentret vid Traficom förbereder sig för att ändra sin verksamhet för uppgifter i enlighet med regleringen ovan.

Den nationella samordningscentrumets verksamhet

I början av 2023 grundades Finlands nationella samordningscentrum (National Coordination Centre Finland, NCC-FI) inom Cybersäkerhetscentret vid Transport- och kommunikationsverket. Dess uppgift är att skapa förutsättningar för den finländska cybersäkerhetssektorn såsom företag, högskolor och forskningsinstitut att delta i internationell forsknings- och utvecklingsverksamhet. Det nationella samordningscentrumet är en del av kompetens- och samarbetsnätverket som bildas av nationella samordningscentrum i Europeiska unionens medlemsstater och Europeiska kompetenscentrumet för cybersäkerhet (European Cybersecurity Competence Centre, ECCC).

Det nationella samordningscentrumet (NCC-FI) fick projektfinansiering för perioden 2023–2024 ur Programmet för ett digitalt Europa, som det kan dela till tredje parter för införande och spridning av moderna cybersäkerhetslösningar och -innovationer. Genom finansieringsprogrammet strävar Europeiska kommissionen efter att öka cybersäkerhetskapaciteten och den strategiska självförsörjningen i sina medlemsländer.

Den första ansökan om finansiellt stöd till tredje parter var öppen 16.6–16.8.2023. Stödet kunde sökas av små och medelstora företag registrerade i Finland. Beslut om den första ansökan om finansieringsstöd som ordnades av det nationella samordningscentrumet fattades 15.11.2023. 13 sökande beviljades totalt cirka 485 000 euro i finansieringsstöd. Totalt fanns 500 000 euro att söka i finansieringsstöd och totalt ansökte man om cirka 633 000 euro i stöd.

Cybersäkerhet

> ”Genom finansieringsprogrammet strävar Europeiska kommissionen efter att öka cybersäkerhetskapaciteten och den strategiska självförsörjningen i sina medlemsländer.

Cybersäkerhetscentret stödde utvecklandet av lagstiftningen

På såväl EU-nivå som nationell nivå har man på ett berömvärt sätt och i allt större utsträckning ägnat uppmärksamhet åt regleringen i fråga om cybersäkerheten. Centrala lagstiftningsprojekt 2023 var bland annat det nationella genomförandet av NIS2-direktivet och samordningen av genomförandet på EU-nivå, slutförandet av förhandlingarna om cyberresiliensakten, förhandlingarna om cybersolidaritetsakten samt beredningen av en ny eIDAS-förordning. Det planeras även ett ökande antal nya uppgifter för ämbetsverket och därmed också för centret i fråga om tillsyn över efterlevnaden av cybersäkerhetslagstiftningen.

Cybersäkerhetscentret stöder som en del av Transport- och kommunikationsverket utvecklandet av lagstiftningen genom att tillhandahålla sin expertis till lagberedningen. Centret gav 2023 tiotals utlåtanden om lagberedningar i EU och i hemlandet samt deltar aktivt i samarbetsgrupper inom sin sektor både när det gäller kvalitativ beredning av lagstiftning och för att säkerställa att den gällande lagstiftningen följs.

Cybersäkerhetscentret styr och övervakar televerksamhetens informationssäkerhet, driftssäkerhet och beredskap samt informationssäkerheten för starka och betrodda elektroniska tjänster samt de leverantörer av digital infrastruktur och tjänster som avses i EU:s direktiv om nät- och informationssäkerhet (NIS-direktivet). Dessutom övervakar centret även genomförandet av skyddet av kommunikationens konfidentialitet vid elektronisk kommunikation. Som en del av Transport- och kommunikationsverket utfärdar centret också föreskrifter som preciserar lagen för aktörer som centret övervakar och ger dagligen medborgare och företag råd om hur regleringen ska följas.

Föreskrifterna uppdateras regelbundet för att motsvara förändringarna i cybersäkerhetsmiljön och den tekniska utvecklingen. Ett exempel på detta är föreskriften om televerksamhetens informationssäkerhet som reviderades 2023 och den reviderade föreskriften utfärdas under 2024.

Tillsynen av hur lagstiftningen efterföljs 2023 genomfördes bland annat genom handläggning av hundratals anmälningar om störningar i funktions- och informationssäkerheten samt genom att utfärda fallspecifika

tillsynsbeslut bland annat om användningen av kakor på webbplatser. Centret genomförde också bland annat inspektioner i teleföretag av passagekontroll i utrustningsutrymmen och landtagningsplatser för sjökablar.

Centrala EU-projekt 2023 i fråga om regleringen var bland annat det nationella genomförandet av NIS2-direktivet och samordningen av genomförandet på EU-nivå, slutförandet av förhandlingarna om cyberresiliensakten, förhandlingarna om cybersolidaritetsakten och flera arbetsgruppsdiskussioner för att stärka skyddet av kritisk infrastruktur.

Trender inom cybersäkerheten år 2024

Hotnivån för cybersäkerheten är fortfarande hög under 2024.

Utsikter för cybersäkerhetens allmänna hotnivå 2024

Under 2024 ser man sannolikt allt fler fall av utpressningsprogram som är allvarligare och mer utvecklade. Detta återspeglas även i Finland, men genom företagens aktiva och omsorgsfulla skydds- och bekämpningsåtgärder och samarbete kan hotet begränsas avsevärt även i fortsättningen.

Fenomenet med utpressningsprogram som tjänsteutbud (Ransomware-as-a-Service, RaaS) kommer att bli vanligare, vilket innebär att aktörer för cyberhot med olika motiv lättare kan utnyttja utpressningsprogram som en del av sin verksamhet. Det uppstår sannolikt även nya versioner av skadliga program och aktörer som sysslar med utpressningsprogram strävar efter att förbättra sina angreppsmetoder och har sannolikt nolldagarssårbarheter som en del av sina operativa verktyg.

Under 2024 kommer cyberbrottslingar i allt större utsträckning att utnyttja teknologier baserade på artificiell intelligens. Artificiell intelligens utvecklas till exempel för analysering av publicerade programuppdateringar för att skapa sårbarheter och metoder för att utnyttja dem. Tekniker för artificiell intelligens utvecklas även för automatisering. När dessa metoder utvecklas kan brottslingar automatiserat söka efter sårbarheter i miljarder nätverksenheter mycket snabbt efter publiceringen av uppdateringar. Detta kan till exempel medföra att kampanjer av aktörer som sysslar med utpressningsprogram blir mycket effektiva.

Kartläggningen av kritiska sårbarheter fortsätter i Finland även 2024. Snabba åtgärder krävs av tiotals, om inte hundratals inhemska organisationer till exempel för att avhjälpa kritiska sårbarheter i nätverksenheter.

På konsumentmarknaden introduceras fortfarande många produkter med bristfälliga informationssäkerhetsegenskaper i snabb takt.

Överbelastningsangrepp mot olika organisationers webbplatser och -tjänster fortsätter aktivt. Genomförande av överbelastningsangrepp kräver ingen särskild teknisk kunskap.
Ett angrepp kan till exempel köpas som en tjänst av brottslingar. Organisationer ska ha beredskap för överbelastningsangrepp som
en del av sin dagliga verksamhet.

Cyberspionage fortsätter att vara aktivt också 2024. Cyberspionage är ett förmånligt och effektivt sätt för en stat som bedriver spionage att inhämta betydande mängder information som är avsedd att vara konfidentiell. Den som råkar ut för cyberspionage märker det nödvändigtvis inte själv. Statliga aktörer strävar genom att utnyttja olika sårbarheter efter att få tillgång till olika konfidentiella uppgifter. I Finland är det Skyddspolisens uppgift att avvärja spionage av främmande stater, också på webben.

Ett av temana i kampanjen Smarta inköp var att påminna om informationssäkra enheter för hemmet.

Älyäostoksiin.fi

Anvisning – Överbelastningsangrepp | Cybersäkerhetscentret

Viktiga ändringar i lagstiftningen

Den ökade regleringen för cybersäkerhet på EU-nivå och nationell nivå fortsätter 2024. En av årets viktigaste frågor med tanke på centrets verksamhet är färdigställandet av den för hösten 2024 planerade nationella implementeringen av det nya direktivet för nät- och informationssäkerhet (det s.k. NIS2). I och med den nya lagen kommer Cybersäkerhetscentret att få nya uppgifter och gör förberedelser för att påbörja dessa under 2024 samt tillhandahålla stöd även till de som centret ska övervaka efter att lagen träder i kraft.

Med tanke på företagen är ett av de första stegen att sätta sig in i informationssäkerhetspraxis på basnivå som publiceras i början av 2024 och som fungerar som konkret handledning för att påbörja genomförandet. Det är viktigt att följa dessa praxis när företagen försöker uppfylla kraven i NIS2-direktivet. Företagen ska vara redo att ändra och effektivisera sina cybersäkerhetspraxis att bättre motsvara dagens digitala hot.

Det är känt att reglering som hänför sig till produkters säkerhet kommer att införas för tillverkare av digitala produkter. Tillämpningen av informationssäkerhetskraven i direktivet om radioutrustning (Radio Equipment Directive, RED) har framflyttats till augusti 2025, vilket ger företag mer tid att förbereda sig på kraven. Direktivet gäller alla enheter som direkt eller indirekt ansluts till internet. Närmare definitioner om överenstämmelse med kraven publiceras under 2024. Cyberresiliensakten (Cyber Resilience Act, CRA) förväntas träda i kraft under 2024. CRA kommer att gälla alla internetanslutna produkter och deras hela livscykel. Tillämpningen av akten förväntas börja etappvis så att skyldigheten att informera om sårbarheter börjar tillämpas 2026 och övriga skyldigheter 2027. Det är därför klokt av tillverkarna att redan nu börja förbereda sig på informationssäkerhetskrav på basnivå. Cyberresiliensakten utmanar tillverkarna att utveckla starka cybersäkerhetspraxis och integrera dessa i sina produktionsprocesser redan på förhand.

Nästa år fortsätter också en av justitieministeriet ledd totalreform av beredskapslagen som Traficom och Cybersäkerhetscentret även i fortsättningen ger sina synpunkter på med tanke på den egna sektorn.

Den teknologiska utvecklingen fortsätter att vara livlig 2024

En av de centrala trenderna 2023 var den snabba utvecklingen av generativ artificiell intelligens. Genom generativa metoder har man producerat realistiska förfalskade bilder, videor och text. Man har allmänt konstaterat att denna utveckling leder till spridning av desinformation och gör det svårare att skilja sanning från fiktion.

Det är sannolikt att man med generativa metoder för artificiell intelligens kan skapa en video i realtid under 2024. Detta gör det möjligt att också skapa videor där ansiktsrörelserna och rösten hos fiktiva eller verkliga personer synkroniseras realistiskt för att skapa ett intryck som är äkta. Det finns mångahanda affärsverksamhetsbehov för att skapa dessa videor med målpersonens samtycke, och det är sannolikt att användningen av dessa snabbt kommer att bli vanligare.

I synnerhet när videor skapas i vilseledande syfte och utan samtycke av målpersonen talar man om så kallade deepfake-videor, på svenska djupförfalskningar eller mer allmänt förfalskade videor. Generering av förfalskade videor i realtid kan ytterligare öka bedrägerimöjligheterna inom flera olika områden. I bedrägerier mot företag kan man använda förfalskade videor till exempel för att redigera företagsledares ansiktsrörelser och röst för att skapa ett intryck av att det är ett äkta meddelande.

Samarbete bland industrin, forskare och myndigheter är centralt när det gäller att avvärja förfalskat innehåll. Tjänster som utvecklas ska från ett så tidigt skede som möjligt också bedömas ur missbrukens synvinkel och man ska försöka skapa olika sätt att observera och förhindra missbruk. Gemensamma ansträngningar kan leda till bättre identifieringsmetoder och skyddsmekanismer. Man har redan utvecklat till exempel avancerade teknologier för identifiering av förfalskade videor. AI-baserade system försöker upptäcka tecken på att en video eller en bild har genererats, och de försöker skilja autentiskt innehåll från förfalskat innehåll. Man har även framfört olika tekniker som försöker säkerställa innehållets autenticitet.

När tekniken för att modellera ansikten och röster blir vanligare kan trovärdiga förfalskade videor även göras av privatpersoner. Förfalskade videor av detta slag kan underlätta identitetsstölder och olika bedrägerier där en individs identitet används för bedrägerisyften.

I bedrägerier riktade mot privatpersoner kan förfalskade videor som modellerar verkliga eller fiktiva personer ge ett intryck av en mer personlig interaktion mellan bedragarna och offren. Detta kan öka offrens känslomässiga kontakt med bedragaren och göra dem mer utsatta för bedrägerier. I synnerhet i släkt- eller romansbedrägerier börjar man sannolikt använda förfalskad röst och videobild. Bedragarna kan till exempel framföra fiktiva kriser eller berättelser av olika slag i hopp om ekonomiskt stöd. Med generativa tekniker för artificiell intelligens kan man också enkelt skapa trovärdiga förfalskningar ur olika dokument för att stödja bedrägeriberättelser. Det är sannolikt att man alltid kommer att hitta på nya typer av bedrägerier när de föregående lärt oss att vara försiktiga.

Förfalskade videor kan användas som en del av mer omfattande informationspåverkanskampanjer. Sådana kampanjer kan sträva efter att påverka den allmänna opinionen, sprida desinformation eller skapa förvirring i samhället.

Ökade medvetenhet om förekomsten av förfalskade innehåll och eventuella risker kunder uppmuntra allmänheten att vara försiktig och kritisk när det gäller digitalt innehåll. Även lagstiftningsåtgärder kan främja ansvarsfull användning av artificiell intelligens och ställa strängare krav på utvecklare av generativa modeller. Den tekniska utvecklingen kännetecknas av en kontinuerlig konkurrens mellan utvecklare och säkerhetsexperter. Samtidigt som säkerhetsåtgärder vidtas, utvecklar också angriparna nya sätt att kringgå dem.

Metoder för artificiell intelligens och i synnerhet generativ artificiell intelligens kommer även att utvecklas på andra sätt i försvarssyfte. De förväntas i synnerhet ge bättre verktyg för upprätthållande av säkra systeminställningar och analys av informationssäkerhetsincidenter samt möjligheter att reagera på automatiserade säkerhetshot. År 2024 kommer man att se olika lösningar för observation och utredning av informationssäkerhetsincidenter med hjälp av artificiell intelligens.

Användning av artificiell intelligens inom programvaruproduktion kan påverka cybersäkerheten på många sätt i de system som skapats. Utöver egentlig programvaruproduktion har de använts till exempel för att skapa testfall för att underlätta utvecklingen och upprätthållandet av systemet. I och med utvecklingen av modeller för artificiell intelligens kunde de hjälpa utvecklare att producera säkrare kod och identifiera potentiell riskbenägen kod eller dålig praxis. På motsvarande sätt kan de också bidra till att identifiera sårbarheter och informationssäkerhetsbrister i programvaror.

” Samtidigt som säkerhetsåtgärder vidtas, utvecklar också angriparna nya sätt att kringgå dem.

Hantering av informationssäkerhetskompetens framhävs ytterligare

Cyberbrott och -brottslighet ändrar ständigt sin form. Till exempel de teknologier och tekniker som används i olika bedrägerier och nätfiskekampanjer utvecklas och blir ständigt allt mer sofistikerade och listigare. Det blir allt svårare för vem som helst att identifiera dessa.

I takt med att samhället i rask takt digitaliseras är det en viktig medborgarfärdighet att förvärva och ständigt utveckla informationssäkerhetsfärdigheter. Enskilda medborgare är allt oftare föremål för cyberangrepp såsom nätfiske, dataintrång, försök till kapning av konton i sociala medier, utpressningsprogram och bluffmeddelanden. Detta inkluderar även olika former av informationspåverkan, till exempel spridning av desinformation. Därför är det viktigt att man satsar på att upprätthålla och utveckla medborgarnas informationssäkerhetskompetens samt deras medie- och teknologikunskap.

Medborgarnas cybersäkerhetsfärdigheter varierar mycket. En del behöver hjälp med grundläggande saker, till exempel lösenord och programuppdateringar samt identifiering av bedrägerier. Andras informationssäkerhetsfärdigheter är å andra sidan på en utmärkt nivå.

Inom cybersäkerhet handlar det även om förtroende. Om folk inte litar på de elektroniska tjänster eller produkter som ett företag eller en organisation erbjuder vill de inte heller använda dem. Ju mer samhället och dess tjänster digitaliseras, desto viktigare är det att ägna uppmärksamhet åt god informationssäkerhet och på att upprätthålla förtroendet. Aktiv, öppen och regelbunden kommunikation bidrar till att upprätthålla förtroendet. Man ska kommunicera öppet och transparent om såväl bra saker som problem. I det digitaliserade samhället bör uppmärksamhet även ägnas åt att delaktigheten förverkligas.

Den offentliga diskussionen om cybersäkerheten handlar i dagens läge mycket om artificiell intelligens och djupförfalskningar (deepfake) som gjorts med hjälp av den. När man talar om hot är det även bra att komma ihåg att man också förbereder sig på dem. På samma sätt som artificiell intelligens möjliggör nya bedrägerier och cyberangrepp, ger den också metoder för att skydda sig mot dem.

Cybersäkerhetscentret stöder cyberfärdigheterna för medborgare på alla informationssäkerhetsnivåer.

Cybersakerhetscentret.fi

Våra kommunikationssakkunniga presenterar hur teknologi möjliggör allt mer bedräglig vilseledning som hjälpmedel för cyberhot och informationspåverkan.

Deepfake: hur gör djupförfalskningar cyberbrottslighet och informationspåverkan effektivare? | Youtube (på finska)

Nyckeltal för vår verksamhet 2023

Varningar
1
(2022: 1 st.)

Bedrägerier
4 963
(2022: 3 519 st.)

Nätfiske[1]
9 266
(2022: 5 787 st.)

Dataläckage
111
(2022: 104 st.)

Data-intrång[2]
1 014
(2022: 1 026 st.)

Dataintrångs-försök[3]
383
(2022: 127 st.)

Automatisk handläggning av fall
209 416
(2022: 188 561 st.)

Informationssäkerhets-incidenter totalt
18 625
(2022: 12 947 st.

Facebook följare
7 190
(2022: 6 939 st.)

X-följare
17 200
(2022: 16 805 st.)

Medie-kontakter
152
(2022: 142 st.)

Kundnöjdhet i fråga om lägesbildsprodukterna
4,3
(2022: 4,3)

1 År 2023 fick vi 3 881 anmälningar om nätfiske av bankkoder.
2 Inkluderar medborgarnas konton i social medier,
3 Störst tillväxt i förhållande till förra året

Transport- och kommunikationsverket Traficoms Cybersäkerhetscenter

PL 320, 00059 TRAFICOM

p. 029 534 5000

Cybersakerhetscentret.fi

Traficoms publikationer 10/2024
ISSN 2669-8757 (elektronisk publikation)
ISBN 978-952-311-909-3

TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret