TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret

Informations-säkerhetens år 2022

Innehåll

Traficoms publikationer 16sv/2023
ISSN 2669-8757 (e-publikation)
ISBN 978-952-311-894-2

Informationsutbyte, samarbete och beredskap – cybersäkerhet skapar vi tillsamman

Efter att 2023 kommit igång ordentligt är det bra att påminna om de viktigaste händelserna under 2022, som var ett exceptionellt år på många sätt.

Förra året steg hotnivån mot cybersäkerheten högre än någonsin tidigare. Förändringen har blivit permanent. Den långvariga ökningen av mängden cyberstörningar planade ut, men cyberstörningarna förändrades i och med kriget i Ukraina och blev ännu allvarligare och mer riktade än tidigare. Bedrägerier, överbelastningsangrepp, skadeprogram och utpressningsangrepp mot organisationers IKT-miljöer samt nätfiske inverkade på vardagen för finländarna och de organisationer som har verksamhet i Finland.

Efter att Ryssland inledde sitt storskaliga angrep mot Ukraina i februari 2022 varnade Cybersäkerhetscentret vid Traficom samt andra myndigheter för en eventuell ökning av mängden cyberhot i olika kanaler. Antalet allvarliga cyberstörningar, exempelvis det betydande antalet fall av utpressningsangrepp, som rapporterades till Cybersäkerhetscentret började också öka i juli 2022. År 2021 konstaterades endast några sådana fall och 2022 registrerades över tio fall i kritiska samhällsfunktioner. I dessa fall bistod Cybersäkerhetscentret de utsatta organisationerna i återhämtningen.

År 2023 fortsätter hotnivån mot cybersäkerheten att vara förhöjd och cybersäkerheten är fortfarande ett viktigt tema i samhället. Cyberhoten intresserar samt väcker mycket offentlig debatt och förståeligt nog även oro. I den här debatten är det viktigt att diskussionen om hoten samt beredskapen för och avvärjandet av dem förs utifrån aktuell och korrekt information. Myndigheterna har förmåga och skyldighet att producera denna information.

I denna översikt behandlas förra årets allmänna händelser och fenomen inom cybersäkerheten i Finland, utvecklingsåtgärder inom cybersäkerheten samt verksamheten vid Cybersäkerhetscentret vid Traficom.

> ”Under 2022 främjades cybersäkerheten på många olika sätt.

År 2022 utvecklades och förbättrades lägesbilden, samarbetet och informationsutbytet i fråga om cybersäkerhet

Cyberhot tar inte hänsyn till gränserna mellan olika länder eller samhällssektorer. Cyberhoten är, liksom övriga nutida hot, till sin karaktär sektorsövergripande och ur myndigheternas synvinkel tväradministrativa. I och med digitaliseringen är sektorerna beroende av varandra, och det är sällan som en störning i dag berör endast ett förvaltningsområde eller en samhällssektor. Att förbereda sig för och svara på moderna hot förutsätter att samarbetet fungerar samt att kopplingarna mellan ledningen, lägesbilden och kommunikationen är i ordning. Beslut måste fattas utifrån korrekt information och en korrekt lägesbild. Samarbetet mellan olika samhällssektorer i fråga om beredskap har långa traditioner i Finland.

År 2022 fortsatte arbetet med att utveckla cybersäkerheten genom att intensifiera samarbetet internt vid och mellan de ministerier och cybersäkerhetsmyndigheter som ansvarar för säkerheten. För att säkerställa samarbetet och informationsutbytet mellan myndigheterna samt producera en gemensam lägesbild tillsattes en separat grupp på ministerienivå våren 2022. Gruppens uppgift är att vid behov stödja statsledningens beslutsfattande vid allvarliga cyberstörningar eller cyberpåverkan. Därtill kompletterades uppgiften för ministerarbetsgruppen för utveckling av digitaliseringen, dataekonomin och den offentliga förvaltningen i mars 2022 beträffande cybersäkerheten och den offentliga förvaltningens beredskap.

Traficom och dess Cybersäkerhetscenter utvecklade fokusområdena för sin verksamhet för att motsvara den förhöjda hotnivån. Nya kompetenser utvecklades för den tekniska observationsförmågan och för tillhandahållandet av snabb hjälp vid allvarliga cyberstörningar. Cybersäkerhetscentret började producera bland annat en ny strategisk lägesbild över cybersäkerheten för statsledningens behov.

Säkerställande av driftssäkerheten och säkerheten för telekommunikationsförbindelserna samt stödjande av teleföretagens beredskap fortsatte att vara ett viktigt mål i styrnings- och övervakningsverksamheten. Under året främjades även flera lagstiftningsprojekt som syftar till att utveckla företagens informationssäkerhet, riskhantering och beredskap samt stödja myndigheternas samarbete inom cybersäkerhet och förbättra förutsättningarna för informationsutbyte.

Under 2022 intensifierade Cybersäkerhetscentret sitt samarbete nationellt och internationellt.

Vi påverkade i nationella och internationella nätverk samt deltog aktivt i beredningen och utvecklingen av lagstiftning. Vi genomförde, samordnade och deltog i flera projekt som utvecklade cybersäkerheten.

I det storskaliga anfall som Ryssland inledde mot Ukraina i februari 2022 har cyberdimensionen spelat en stor roll. Cybersäkerhetscentret har noggrant följt och analyserat de cyberangrepp som setts i Ukraina samt bistått olika sektorer i det finländska samhället i deras förberedelser och beredskap för olika typer av hot som växer fram i cybermiljön. Ett exempel på detta är olika projekt för cyberberedskap med snabba reaktioner, där tjänster för snabba första insatser och en ny strategisk lägesbildsanalys av cybersäkerheten utvecklades. Bland annat den högsta statsledningen får ta del av denna analys. Cybersäkerhetscentret har även haft ett nära samarbete med finländska teleföretag för att säkerställa kommunikationsnätens och -tjänsternas funktion samt beredskapen för olika slags hot.

Inom cybersäkerheten är myndigheternas roller och uppgifter tydliga

I Finland bedrivs det varje dag arbete för att upprätthålla och utveckla cybersäkerheten. Arbetsfördelningen mellan myndigheterna i fråga om cybersäkerheten är tydlig och baserar sig på lagstiftning. Man samarbetar operativt varje dag, och myndigheterna har väl organiserade grupper och verksamhetsmodeller för samordning. Vid cybersäkerhetsstörningar producerar cybersäkerhetsdirektören tillsammans med gruppen på ministerienivå en lägesbild för statsledningen och samordnar situationen. Därtill samordnar kommunikationsministeriet situationen horisontellt med övriga ministerier.

Man utbyter hela tiden information om och delar en lägesbild över cybersäkerheten och cybersäkerhetshoten med samarbetspartner och intressenter i Finland och utomlands. Samarbetet mellan aktörerna samt olika samhällssektorer är intensivt.

Utvecklingen av cybersäkerheten är en kontinuerlig och strategisk verksamhet

Upprätthållande och utveckling av cybersäkerheten kräver satsningar. Det är en långsiktig och strategisk verksamhet som den aktuella lagstiftningen samt cybersäkerhetsstrategin, som trädde i kraft 2019, och programmet för utveckling av cybersäkerhet skapar bra ramar och riktlinjer för. 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.

Beredskapen för och förmågan att svara på cyberhot utvecklas kontinuerligt genom övningsverksamhet och utveckling av regleringen. Prognoser för framtiden tas fram till exempel i arbetet med olika scenarion genom att analysera tekniska och samhälleliga utvecklingstendenser. Utan en uppfattning om framtiden är det svårt att vidta rätt åtgärder proaktivt och i rätt tid. Utveckling av cybersäkerhet är strategisk verksamhet, som baserar sig på en aktuell lägesbild och -analys.

Cybersäkerheten främjas och stöds även på många andra sätt. Som exempel kan nämnas stödet för utveckling av informationssäkerheten, det vill säga den så kallade informationssäkerhetssedeln, som statsrådet beslutade om i slutet av 2022 och som är avsett för företag som är livsviktiga med tanke på samhällets funktioner, Försörjningsberedskapscentralens femåriga programhelhet Digital säkerhet 2030 samt de utvecklingsprojekt som finansieras av finansministeriet ur programmet Genomförandeplanen för digital säkerhet inom den offentliga förvaltningen 2020–2023 (Haukka).

Cybersäkerhetscentret stöder hela samhällets och dess olika sektorers cyberresiliens

Cybersäkerhetscentret vid Transport- och kommunikationsverket Traficom styr och övervakar kommunikationsnätens och -tjänsternas driftssäkerhet och säkerhet, informationssäkerheten för stark autentisering och betrodda elektroniska tjänster samt informationssäkerheten och riskhanteringen hos olika typer av leverantörer av digital infrastruktur och digitala tjänster. Vi var starkt involverade i utvecklingen av både den nationella och internationella regleringen och standardiseringen som gäller för området.

Cybersäkerhetscentret vid Traficom är den myndighet i Finland som har till uppgift att producera en övergripande lägesbild och analys över informations- och cybersäkerheten i samtliga samhällssektorer samt stödja utvecklingen av cybersäkerheten över sektors- och förvaltningsområdesgränserna. Den strategiska lägesbild och analys som vi producerar används på bred front, till exempel i den högsta statsledningens beslutsfattande och inom sektorer som är kritiska för försörjningsberedskapen.

Cybersäkerhetscentret deltar aktivt i det nationella och internationella samarbetet och informationsutbytet beträffande cybersäkerheten. I centrets prognos- och scenarioarbete följer man upp och analyserar i stor utsträckning samhälleliga och tekniska utvecklingstrender som allmänt påverkar cybersäkerheten, till exempel användningen av artificiell intelligens vid cyberangrepp. Verksamheten stöder beredskapen och utvecklingen i fråga om cybersäkerheten inom olika samhällssektorer.

Cybersäkerhetscentret betjänar hela Finland, och en av dess uppgifter är att allmänt informera om cyberhot, exempelvis sårbarheter i olika program som används. Cybersäkerhetscentret producerar och uppdaterar kontinuerligt anvisningar avsedda för såväl medborgarna som olika organisationer där man beskriver hur man till exempel kan förebygga olika typer av informationssäkerhetsincidenter. Cybersäkerhetscentret ger företag, samfund och medborgare råd i frågor om informations- och cybersäkerhet samt bistår förundersökningsmyndigheter i utredningen av cyberbrott. På centrets webbplats publiceras varje vecka Cybersäkerhetscentrets veckoöversikt, där man berättar om de senaste faktorerna och observationerna som påverkar cybersäkerheten. I översikten Cybervädret, som publiceras varje månad, undersöks mer långsiktiga trender inom cybersäkerhet. På centrets webbplats finns även anvisningar för alla om upprätthållande och utveckling av cybersäkerhetsfärdigheter för vardagen.

Cybersäkerhetscentret bedömer att enbart dess förebyggande av informationssäkerhetsincidenter och åtgärder för att hjälpa medborgarna varje år ger samhället en stor nettonytta i euro.

> ” Cybersäkerhetscentret skapar en omfattande lägesbild av cybersäkerheten.

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 många av de tjänster som är viktiga och kritiska för samhället.

Utan den privata sektorns tjänsteleverantörer skulle det i praktiken inte finnas någon elektronisk kommunikation – åtminstone inte tillgänglig för alla medborgare. Exempelvis 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.

Inom cybersäkerhet handlar det även om förtroende

Inom cybersäkerhet är det även fråga om människornas förtroende för samhället samt dess institutioner och tjänster. Om man inte litar på tjänsterna och informationssäkerheten i dem vill man inte heller använda dem. Det är viktigt att upprätthålla och stärka förtroendet. Förtroendet är det lim som håller ihop vårt samhälle. Hit hör även förtroendet för digitala tjänster och cybersäkerheten. Genom att göra rätt saker och öppet kommunicera om dem kan vi bidra till att förtroendet upprätthålls. Det är även viktigt att prata om problem och fel på ett öppet och transparent sätt.

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. Sådan debatt stöder och främjar samhällets krismedvetenhet och resiliens. Cybersäkerheten utvecklas varje dag, och verksamheten och verksamhetssätten ändras enligt förändringarna i hotmiljön. Hot som växer fram i cybermiljön analyseras kontinuerligt och man svarar på dem.

Under 2022 pågick flera kriser samtidigt. Förändringen i säkerhetsmiljön, coronapandemin, energikrisen, hotet om ekonomisk nedgång samt klimatförändringen berörde var och en av oss. De ekonomiska konsekvenserna av kriserna lyftes snabbt fram i den offentliga debatten, men lika viktigt är det att även ägna uppmärksamhet åt de sociala och samhälleliga konsekvenserna av dem. Dessa konsekvenser kan visa sig först efter lång tid.

När det handlar om säkerhet är det även fråga om en känsla. Människornas tolkningar och upplevelser av risker och kriser kan skilja sig avsevärt från myndigheternas och andra aktörers uppfattningar. Detta informationsbehov bör myndigheterna och andra samhälleliga aktörer svara på genom att lyssna och diskutera samt genom aktiv, rättidig och öppen kommunikation. Detta gäller även cyberhot.

Cyberhot berör hela samhället på ett konkret sätt, från individen till samhället som helhet. Störningar i digitala nät eller elektroniska tjänster påverkar vår vardag. Ju mer och långvarig en störning i vardagen är, desto större möjlighet har den att påverka samhällets mentala resiliens. I beredskapen för cyberhot och när man pratar om sådana är det även viktigt att komma ihåg dimensionen mental resiliens.

Till sist är det värt att påminna om att utveckling av cybersäkerheten är som ett ultramaraton. Skillnaden jämfört med en löptävling i den verkliga världen är att mållinjen i cybervärlden alltid flyttas och att nya medtävlare kan hoppa ur buskarna för att delta i loppet. För att vi ska hänga med i tempot och lyckas behövs uthållighet, korrekta och lämpliga verktyg, systematik och strategitänkande, samarbete med servicetrupperna och andra partner samt framförhållning. Vi känner till banprofilen och var de andra löparna befinner sig. Dessutom vet vi hur vi ska anpassa farten, servicen och våra steg enligt det. Det gjorde vi bra under 2022. Mål är också detsamma för det här året och nästa år.

Informations-säkerhetens år 2022

Hotnivån steg under 2022

Coronapandemin och det storskaliga anfallet mot Ukraina som Ryssland inledde i februari 2022 påverkade säkerhetsläget även i Finland. Under 2022 förändrades vår säkerhetsmiljö avsevärt. Myndigheter såsom Skyddspolisen varnade under våren för möjligheten att det kommer att riktas omfattande hybridpåverkan mot det finländska samhället och dess olika sektorer. Skyddspolisen tog även ställning till de aktörer som stod bakom en del av cyberstörningarna. Vi uppmanades att ägna uppmärksamhet åt att förbereda oss för och svara på i synnerhet cyberangrepp och informationspåverkan. Det gjorde vi också. Beträffande cybersäkerheten satsade man på utveckling av beredskapen inom samhällets olika sektorer. Cybersäkerhetscentret bistod organisationerna i detta arbete.

Under 2022 ökade mängden utpressningsprogram, riktat nätfiske och skadlig trafik mot såväl statsförvaltningen som organisationer som är kritiska för försörjningsberedskapen. Även sättet att genomföra angreppen förändrades. På grund av förändringen uppmärksammade och informerade Cybersäkerhetscentret i september om att hotnivån mot cybersäkerheten för första gången höjts. Detta samordnades med Skyddspolisen. Cybersäkerhetscentret bedömer att Finland har klarat den höjda hotnivån bra – bland annat tack vare beredskapskulturen och det öppna diskussionsklimatet mellan myndigheterna.

Kriminellas verksamhet är mycket opportunistisk och de följer noggrant med sin tid. Till exempel under pandemin förekom det bedrägeriförsök där man försökte få människor att lämna ut sina uppgifter med hjälp av teman och ämnen i anknytning till viruset. Även olika staters politiska lösningar, förändringar i säkerhetsmiljön och företagens beslut kan aktivera brottslingar att rikta angrepp mot finländska organisationer.

Det är även bra att komma ihåg att även om ett cyberangrepp inte skulle rikta sig direkt mot Finland, kan det uppstå återverkningar, eftersom de digitala systemen är globalt kopplade till varandra.

> ”Finland har klarat den höjda hotnivån bra.

Mängden överbelastningsangrepp ökade klart i slutet av året

Under 2022 ökade i synnerhet antalet överbelastningsangrepp mot finländska organisationer och företag. Klart fler sådana anmäldes till Cybersäkerhetscentret än år 2021. En del av ökningen berodde dock även på den offentliga debatten och den sänkta tröskeln för att anmäla som den ledde till.

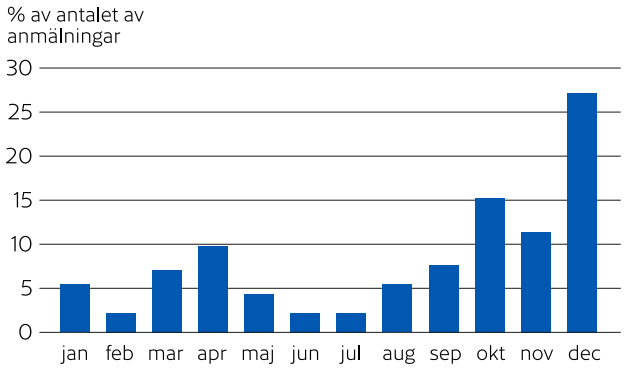
Under 2022 visade överbelastningsangreppen tydliga tecken på hacktivism och kopplingar till politiska ideologier. Även om hacktivismen som fenomen inte är något nytt, var överbelastningsangrepp som ställningstaganden mer synliga i offentligheten än under tidigare år.

Överbelastningsangrepp har förekommit länge runt om i världen, men år 2022 utvecklades de mer till metoder för cyber- och informationspåverkan. Exempel på detta var angrepp som riktade sig mot webbtjänster som medborgarna använder, och genom att förhindra tillträdet till dessa var det möjlighet för den som genomförde angreppet att i offentligheten försöka skapa en bild av ett allvarligare angrepp än det i verkligheten var.

Antalet överbelastningsangrepp som genomfördes som ställningstagande till följd av kriget i Ukraina ökade. Även många andra internationella politiska eller andra betydande händelser aktiverade hacktivisterna att genomföra överbelastningsangrepp. De mest synliga fallen bland de angrepp som riktades mot Finland var de angrepp som genomfördes av pro-ryska hacktivistgrupper, till exempel NoName057(16) och Killnet. Målen var i synnerhet aktörer inom statsförvaltningen, hälso- och sjukvårdssektorn, finanssektorn, trafik- och logistiksektorn samt mediebranschen, där avbrott i tjänsterna fick direkt synlighet för medborgarna, även om de inte hade någon effekt på organisationernas interna system och effekterna på de externa tjänsterna i huvudsak var kortvariga.

Överbelastningsangrepp har redan i många år varit en del av vardagen i Finland. Över 10 000 angrepp konstateras årligen. Det kräver ingen särskild teknisk kompetens att genomföra ett överbelastningsangrepp, utan man kan beställa angrepp av brottslingar som en kommersiell tjänst. Ett överbelastningsangrepp är en effektfull metod, och att genomföra ett sådant ger lätt publicitet. Olägenheten till följd av ett angrepp är kortvarig, och de orsakar sällan någon verklig skada. Som sätt att påverka placerar sig överbelastningsangrepp i en gråzon mellan cyber- och informationspåverkan.

Cybersäkerhetscentrets behandlade anmälningar av överbelastningsangrepp 2022



Under 2022 genomfördes överbelastningsangrepp även mer ihärdigt än tidigare, och angriparen kunde bland annat variera tekniken allt efter som bekämpningsåtgärder vidtogs. Cybersäkerhetscentret upprätthöll en lägesbild över överbelastningsangreppen, bistod organisationer i bekämpningen av dem och delade information om deras verkliga effekter i offentligheten. Anmälningarna om överbelastningsangrepp till Cybersäkerhetscentret från olika organisationer ökade under året, och även mot ihärdiga angrepp med olika metoder lyckades man genomföra skyddsåtgärder för att begränsa angreppen och förhindra deras effekt. I december anmäldes en fjärdedel av hela årets överbelastningsangrepp i Finland till Cybersäkerhetscentret.

Finländska organisationer blev oftare än tidigare offer för utpressningsprogram

År 2022 fick Cybersäkerhetscentret fler anmälningar än året innan från organisationer som blivit utsatta för utpressningsprogram. I offentligheten var fallen med till exempel Finska Notisbyrån STT, Wärtsilä Oyj Abp, Vahanen Oy och Uponor Oyj framträdande. Utpressningsprogrammen ökade även internationellt. Även till Finland kom fenomenen och trenderna från andra länder. År 2022 berörde de globala fallen Finland mer än tidigare, och i offentligheten kopplades också en del av angreppen till det världspolitiska läget.

Under året var spridningen av utpressningsprogram i Finland mer riktad än tidigare, och de skadeprogram som identifierades i de fall som observerades i Finland var i aktiv användning även internationellt. Under 2022 ökade antalet fall med utpressningsprogram i synnerhet på sommaren, men på hösten minskade antalet anmälningar om sådana. Mot slutet av året ökade fallen igen. Under sommaren riktades angrepp med utpressningsprogram som var tydligt riktade mot en målorganisation mot stora och betydande företag, och i slutet av året utsattes även aktörer inom kommunsektorn.

Även om föremålen för angreppen var också betydande storföretag och organisationer som är kritiska för försörjningsberedskapen, var de metoder som användes i angreppen ganska vanliga. En stor del av angreppen med utpressningsprogram genomfördes med hjälp av nätfiskemeddelanden som skickades per e-post. Även bristen på andra vanliga skyddsmetoder såsom god lösenordspraxis eller programuppdateringar utnyttjades i angreppen med utpressningsprogram.

> ”Under året var spridningen av utpressningsprogram i Finland mer riktad än tidigare.

Finska Notisbyrån STT fick år 2022 erkännandet Vägvisare för informationssäkerheten för sin öppna kommunikation och sitt agerande när byrån 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.

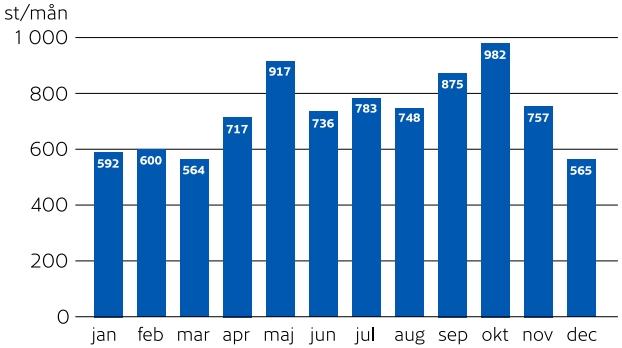
Nätfiske och bedrägerier var en del av vardagen även år 2022

Försök till nätfiske och bedrägerier fortsatte aktivt även under 2022. Under året skickades meddelanden i till exempel olika bankers och myndigheters namn, där man försökte få människor att lämna ut sina bankkoder eller sina kreditkorts- eller personuppgifter till bedragare. Antalet kapningar eller försök till kapningar av konton i sociala medier som rapporterades till Cybersäkerhetscentret fortsatte att öka. Särskilt skadliga har kapningar av konton i sociala medier visat sig vara för personer som får sin huvudsakliga utkomst via en social mediekanal.

År 2022 kännetecknades försöken till nätfiske och bedrägerier av nya tillvägagångssätt. I bedrägerierna är vissa grundläggande tillvägagångssätt dock fortfarande ofta tydliga. Att hänvisa till att det är brådskande, hota eller utge sig för att vara en pålitlig aktör är grundläggande metoder som genomgående används vid bedrägerier. Brottslingar har även riktat nätfiske och bedrägerier beroende på målet, till exempel har vd-bedrägerier och faktureringsbedrägerier i vanlig ordning riktats mot företag under året.

Exempel på de nya tillvägagångssätt som förekommit år 2022 kan nämnas en omfattande bedrägerikampanj som syftade till att byta ut kontonumret för lönebetalning mot bedragarens kontonummer. Samma bedrägeri har observerats även tidigare, men den här gången försökte man genomföra det systematiskt. Med hjälp av ett liknande bedrägeri försökte bedragare överföra hyresbetalningar till sig själva i en sms-kampanj i början av 2023. År 2022 spred sig dessutom utpressningsbedrägerier med polistema från utlandet till Finland. I dokumentbilagor med färgglada stämplar och officiella titlar som förekommit redan tidigare i Europa hotade man med grova anklagelser och påföljder om offret inte betalar lösen i en virtuell valuta. Bedragarna försökte öka bedrägeriets trovärdighet genom att använda Bollförbundets logotyp i en polismyndighets dokument. Likaså har ett nytt större fenomen i början av 2023 varit fiske efter kopior av identitetshandlingar och via det fiske efter personuppgifter för eventuella identitetsstölder.

Cybersäkerhetscentrets behandlade anmälningar av bedrägerier och nätfiske 2022



Beträffande sårbarheter var 2022 lugnare än de senaste åren

Man kommer ihåg 2021 för dess många sårbarheter med globala effekter, och vi publicerade också varningar om några av dem. Under 2022 kunde enskilda sårbarheter med mycket stor påverkan på samhället undvikas. Under 2022 publicerade vi tio sårbarhetsmeddelanden färre än under de två föregående åren.

Nya sårbarheter hittas ständigt. Man försöker även utnyttja gamla sårbarheter vid försök till utnyttjande av sårbarheter. Cybersäkerhetscentret har tagit emot anmälningar där flera år gamla sårbarheter har utnyttjats av kriminella. Bortglömda uppdateringar eller bristfälliga korrigeringar kan utsätta en organisation för många olika slags hot. Organisationerna borde också identifiera sina sårbara system och hålla programmen uppdaterade.

Vi publicerar i genomsnitt 1–3 varningar per år, och den enda varningen under 2022 gällde skadeprogrammet FluBot. Under 2021 publicerades totalt fem varningar, vilket är betydligt fler än genomsnittet.

Kommunikationsnäten fungerade stabilt i Finland under 2022

År 2022 fungerade kommunikationsnäten stabilt i Finland. Det inträffade klart färre serviceavbrott än året innan, och allvarliga avbrott och konsekvenser kunde undvikas. Vid enstaka avbrott uppstod tillfälliga störningar i regionala tjänster eller i nödtrafiken, men avbrotten var kortvariga. Antalet funktionsstörningar i allmänna kommunikationstjänster minskade sammanlagt med 38 procent jämfört med 2021.

Myndigheterna har ett nära samarbete med de finländska teleföretagen beträffande byggandet av dataförbindelserna och säkerställandet av nätens funktion. Regleringen som styr byggandet bidrar till att säkerställa kommunikationsnätens funktion i olika situationer.

Finlands dataförbindelser inom landet och till utlandet är certifierade och krypterade på många olika sätt. Störningar i förbindelserna är dock alltid möjliga. Vid eventuella störningar styrs och hanteras datatrafiken via andra kablar eller backupsystem. Förfarandet är mycket automatiserat, varvid användaren inte ens märker att det är störningar i kommunikationsnäten.

Försök till cyberspionage genomfördes fortsättningsvis aktivt

I likhet med året innan fortsatte försöken till cyberspionage aktivt under 2022. Finländska organisationer var kontinuerligt föremål för verksamhet som syftade till att identifiera vilka tjänster som används och hitta olika sårbarheter eller svaga lösenord. Sårbara nätenheter och -tjänster är intressanta inom cyberspionage, eftersom det via dem är möjligt att komma åt konfidentiell information och kommunikation eller ta sig in i andra system. Därtill utnyttjas riktade skadliga e-postmeddelanden fortfarande allmänt inom cyberspionage. En del av verksamheten tyder på verksamhet av statliga aktörer utifrån myndighetskällor samt offentliga, kommersiella eller andra källor.

Rysslands anfall mot Ukraina syntes under året på många olika sätt inom cyberspionage och -påverkan. I Ukraina upptäcktes under året till exempel flera nya skadeprogram som krypterar uppgifter samt olika nätfiskekampanjer och kampanjer för spridning av skadeprogram. På andra håll i Europa har cyberspionage riktats mot till exempel aktörer med anknytning till kriget eller till humanitär hjälp. Ett exempel på stora konsekvenser av cyberåtgärder även utanför Ukraina under krigstiden var störningen i satellittjänsten Viasat.

> ”I likhet med året innan fortsatte försöken till cyberspionage aktivt under 2022.

Statliga aktörer utnyttjar fortfarande sårbara routrar i hem och småföretag samt servrar för webbaserad datalagring som en del av angreppsinfrastrukturen. Uppdaterade eller bristfälligt skyddade apparater som kan nås via internet är också mer allmänt utsatta för illvilliga åtgärder, vilket håller på att bli ett ökande problem. Sårbara apparater utnyttjas inte nödvändigtvis mot användarna av dem, utan genom att utnyttja apparaterna kan cyberangrepp mot nationella mål genomföras mer obemärkt.

GPS-störningar rapporterades till Traficom

Rysslands anfallskrig mot Ukraina orsakade stora ändringar i flygrutterna när Rysslands luftrum stängdes. Störningar observerades i luftfartygens satellitnavigeringssystem, särskilt i närheten av konfliktområdena. Europeiska unionens byrå för luftfartssäkerhet EASA publicerade en nyhet om ämnet i mars. Också i Finland publicerades ett NOTAM-meddelande i början av mars för att varna alla piloter om GPS-störningar. Meddelandet återkallades den 15 mars 2022.

År 2022 fick Traficom 65 anmälningar om avbruten eller försvagad GPS-signal under flygning av luftfartyg i Finland. Under de tidigare coronaåren var antalet anmälningar 8 st. år 2021 och 27 st. år 2020. Under åren 2017–2019 mottog vi sammanlagt 9 anmälningar. Traficom fick 1 327 anmälningar om GPS-störningar av finländska luftfartyg utanför Finland. Uppföljning av antalet störningssituationer inom luftfarten och internationell hantering av frågan handhas av EASA, Eurocontrol och internationella teleunionen ITU. För händelserapporter inom luftfarten gäller specifika krav på EU-nivå, bland annat för anmälarens integritetsskydd. Händelserapporterna är även sekretessbelagda enligt lagen om offentlighet i myndigheternas verksamhet. Under år 2022 har Traficom inte fått några anmälningar om GNSS-störningar i anknytning till satellitradionavigering från markbaserade aktörer inom transportsektorn.

Antalet markbaserade radiostörningar har minskat

Antalet markbaserade radiostörningar har minskat generellt. Under år 2022 anmäldes sammanlagt 86 radiostörningar till Traficom, varav 32 förutsatte en utredning på fältet. Under år 2021 anmäldes 115 störningar. Av radiostörningarna som anmäldes under år 2022 var 11 förknippade med satellitradionavigering (GNSS). Största delen av dessa var anmälningar om orimligt GNSS-värde från enskilda medborgare, som handlade om till exempel att en sportklocka, bilnavigator eller kartplotter visat till fel plats.

I sin övervakning upptäcker Traficom regelbundet små störsändare (jammer) i hela landet. Under år 2022 gjorde Traficom 422 observationer av störsändare.

Året 2022 för Cybersäkerhetscentret vid Traficom

Beredskapen effektiviserades och samarbetet intensifierades

På grund av förändringen i säkerhetsmiljön och den höjda hotnivån mot cybermiljön effektiviserade myndigheterna beredskapen och intensifierade samarbetet med sina samarbetspartner både i Finland och utomlands. Beredskapsnivån höjdes hos myndigheterna, den offentliga förvaltningen och aktörer inom kritisk infrastruktur. Våren 2022 gav Cybersäkerhetscentret ledningen för organisationer som är kritiska för försörjningsberedskapen preciserande anvisningar och stöd, så att de har kunnat effektivisera beredskapen och kontinuitetshanteringen. Även Skyddspolisen uppmanade företag att förbereda sig för hotet om cyber- och informationspåverkan.

Under 2022 intensifierades samarbetet mellan olika nätverk för informationsutbyte samt produktion och delning av uppgifter om lägesbilden, och samtidigt satsade man på utbyte av information och erfarenheter i realtid. Samarbetet med teleföretagen fortsatte för att säkerställa funktionen hos de finländska näten och tjänsterna. I arbetet utnyttjades bland annat observationer och lärdomar från Ukraina för att skydda kommunikationsinfrastrukturen.

Samarbetet internt vid och mellan de ministerier och cybersäkerhetsmyndigheter som ansvarar för cyberskyddet intensifierades ytterligare under 2022. För att säkerställa samarbetet och informationsutbytet mellan myndigheterna samt producera en gemensam lägesbild tillsattes en separat grupp på ministerienivå våren 2022. Gruppens uppgift är att vid behov stödja statsledningens beslutsfattande vid allvarliga cyberstörningar eller cyberpåverkan.

Nätverkssamarbetet utvecklades år 2022

Kontinuerligt informationsutbyte är en viktig del av Cybersäkerhetscentrets verksamhet och ett av våra viktigaste serviceuppdrag. Vi deltar i flera internationella samarbetsgrupper, och i Finland underlättar vi informationsutbytet inom samtliga samhällssektorer som är kritiska för försörjningsberedskapen. Information byts ut om såväl högaktuella cyberhot som beredskap och hantering av cybersäkerheten.

I Finland är några av de viktigaste nätverken för centret ISAC-grupperna för utbyte av information (information sharing and analysis centre). De är konfidentiella och självständiga grupper som består av organisationer inom en viss bransch. Det finns grupper inom följande branscher: livsmedelsproduktion och -distribution, energi, finans, IKT, media och vattenförsörjning samt ISP, kemisk industri och skogsindustri, logistik och transport, social- och hälsovården samt statsförvaltningen. ICT-ISAC grundades hösten 2022 på uppmuntran av företag inom branschen. Dessutom har användarna av Cybersäkerhetscentrets observations- och varningstjänst HAVARO en egen grupp för informationsutbyte.

Under 2022 var de största temana som behandlades i ISAC-grupperna effekterna av kriget i Ukraina på cybersäkerheten, EU:s NIS2- och CER-direktiv samt DORA-förordning, och samhällets beroende av IKT-tjänster som produceras utomlands. Ämnena diskuterades på ISAC-gruppernas möten, och man genomförde även separata enkäter bland medlemmarna i grupperna. Den insamlade informationen använde Cybersäkerhetscentret i skapandet av den nationella lägesbilden över cybersäkerheten, och frågorna rapporterades även offentligt. Genom att delta aktivt i samarbetet får medlemmarna i informationsutbytesgrupperna även själva aktuell information av jämlikar.

Samarbetet mellan operatörerna och Cybersäkerhetscentret, som inletts 2021, ledde till utfärdandet av en ny rekommendation i början av 2022 om olika metoder för att förhindra förfalskning av uppringarens nummer och undvikande av bedrägerisamtal till mottagare i Finland. Målet är att förhindra användning av finländska telefonnummer i internationell cyberbrottslighet och minska mängden bedrägerisamtal från utlandet. Enligt Centralkriminalpolisen har mängden förlorade euron till följd av bedrägerisamtal också minskat avsevärt jämfört med tidigare år.

Det internationella samarbetet ökade och fortsatte att vara intensivt

Målet med internationellt samarbete är att stödja i synnerhet skapandet av en nationell och internationell lägesbild över cybersäkerheten samt genom det främja uppnåendet av målen för cybersäkerheten i Finland. Det internationella ömsesidiga informationsutbytet är ett livsvillkor för att upprätthålla och utveckla cybersäkerheten på nationell nivå. Information eller varningar från internationella nätverk eller andra stater om cyberangrepp eller exempelvis sårbarheter i informationssystem kan spela en kritisk roll med tanke på den nationella beredskapen.

Under 2022 intensifierades och utvecklades det internationella samarbetet på olika nivåer. Det internationella samarbetet som helhet kännetecknades under 2022 av i synnerhet kriget i Ukraina och det ökade behovet av informationsdelning mellan olika partnerländer. De internationella samarbetsnätverken inom cybersäkerhet visade även sin praktiska förmåga att anpassa sig också snabbt till förändrade situationer i säkerhetsmiljön.

Finland agerar aktivt i internationella organisationer, institutioner och nätverk. I det operativa samarbetet framhävs betydelsen av etablerade samarbetsgrupper inom olika geografiska områden som baserar sig på förtroende. Några av de viktigaste samarbetsgrupperna är NCC-gruppen för de nordiska länderna (Nordic Cert Cooperation), sammanslutningen EGC (European Governmental Certs), som utgörs av vissa europeiska länder, samt det globala nätverket International Watch and Warning Network. Dessutom bedrivs omfattande internationellt samarbete inom olika sektorer, där även Cybersäkerhetscentret deltar. Ett exempel på sådant samarbete är samarbetsgruppen för de nordiska ländernas finansinstitutioner, Nordic Financial Cert.

Även samarbetet på EU-nivå utvecklas kontinuerligt. Cybersäkerhetscentret deltog aktivt i verksamheten för nätverket CSIRT, som utgörs av de nationella cybersäkerhetscentren i EU:s medlemsstater och samlar in en teknisk och operativ lägesbild över cybersäkerheten inom EU. Under 2022 utvecklades samarbetet på en mer strategisk nivå inom EU inom i synnerhet nätverket CyCLONe, som har som mål att producera bland annat en lägesbild och en analys för rådets cyberarbetsgrupp vid främst omfattande krissituationer som berör cybersäkerheten. Vid sidan om EU:s nätverk intensifierades de finländska myndigheternas samarbete även med Natos olika cybersäkerhetsnätverk under 2022.

Cybersäkerhetscentret deltar i Europeiska unionens cybersäkerhetsbyrån Enisas organ och expertgrupper, och fungerar som en nationell kontaktpunkt för Enisa. Vi är också med i verksamheten för NATO CCDCOE, som är Natos kompetenscenter för cyberförsvar i Tallinn.

Vid sidan om de samarbetsnätverk som lyder under reglering eller etablerade institutioner deltog Cybersäkerhetscentret aktivt i verksamheten och samarbetet i flera andra internationella nätverk, exempelvis cybersäkerhetssamarbetet mellan de nordiska länderna. Verksamheten i de nämnda internationella nätverken baserar sig i stor utsträckning på förtroendet mellan de deltagande staterna. I utvecklingen av regleringen utbyter man aktivt lärdomar och information med de nordiska systerämbetsverken och som en del av mer omfattande samarbetsforum inom EU.

Vid sidan om utvecklingen av det operativa samarbetet har olika arbetsgrupper inom EU behandlat ett rekordstort antal initiativ eller projekt med anknytning till cybersäkerhet under 2022. De viktigaste av dem har varit bland annat främjandet av författningshelheter som gäller dataskydd vid elektronisk kommunikation samt identifieringstjänster, färdigställandet av NIS2-direktivet, förhandlingar gällande cyberresiliensakten och ett flertal samarbetsgruppsdiskussioner för att stärka skyddandet av kritisk infrastruktur. Cybersäkerhetscentrets sakkunniga deltog intensivt i utvecklingsprojekt, förhandspåverkan och utarbetandet av regelverk inom cybersäkerheten på EU-nivå. Även den internationella övningsverksamheten var aktiv under 2022. Under 2022 betonades även den strategiska nivån och övning av beslutsprocesser i krissituationer ännu mer än tidigare i övningsverksamheten.

Samhällets säkerhet främjades genom projekt för utveckling av cybersäkerheten och den digitala säkerheten

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. De utvecklingsprojekt som finansieras av Försörjningsberedskapscentralen finansieras ur centralens program Digital säkerhet 2030 och följer de mål som ställts upp i programmet. Under de senaste åren har man kunnat utöka utvecklingsarbetet inom cybersäkerhet, när även finansministeriet har deltagit i finansieringen och stödjandet av dessa utvecklingsprojekt inom cybersäkerhet. De utvecklingsprojekt som finansieras av finansministeriet finansieras ur ministeriets program Genomförandeplanen för digital säkerhet inom den offentliga förvaltningen 2020–2023 (Haukka).

Föremålet för de utvecklingsprojekt som finansieras och stöds av Försörjningsberedskapscentralen är de företag som är livsviktiga för samhället och deras cybersäkerhet, medan föremålet för de projekt som finansieras av finansministeriet är aktörer inom den offentliga förvaltningen, i huvudsak aktörer som är livsviktiga för samhället, och deras cybersäkerhet. De gemensamma målen för de utvecklingsprojekt som finansieras av Försörjningsberedskapscentralen och finansministeriet är att erbjuda ny information, verktyg och tjänster som ska hjälpa livsviktiga aktörer inom både den privata och den offentliga sektorn att förbereda, upprätthålla, utveckla och förbättra sin cybersäkerhet samt genom det hela samhällets cybersäkerhet och säkerhet. Enligt finansministeriet har man genom att involvera sig i projekten för utveckling av cybersäkerheten och intensifiera samarbetet åstadkommit betydande synergier och besparingar, när den information samt de verktyg och tjänster som utvecklingsprojekten resulterat i har kunnat utnyttjas korsvis i utvecklingen och förbättringen av cybersäkerheten inom såväl den privata som den offentliga sektorn. Det har inte heller funnits något behov av att genomföra samma projekt separat för den privata och den offentliga sektorn.

Utvecklingen av övningsverksamheten, situationsmedvetenheten och prognosarbetet fortsatte även under 2022

När man förbereder sig för och svarar på olika störningssituationer är det viktigt att förbindelserna mellan ledningen, kommunikationen och lägesbilden fungerar samt att rollerna och ansvaren är tydliga och inövade. År 2022 fortsatte arbetet med att utveckla situationsmedvetenheten exempelvis genom att utveckla prognosverksamheten i verksamhetsmiljön och genom projektet Cyberklimatet. Syftet med projektet är att utveckla Cybersäkerhetscentrets förmåga att utnyttja data och information för att skapa en nationell lägesbild över cybersäkerheten, skapa nya tjänster och verksamhetsmodeller samt svara på cybersäkerhetshot och -avvikelser.

I prognosarbetet fördjupade vi oss i användningen av artificiell intelligens vid cyberangrepp och brottslighet samt bedömde vi när och i vilken form effekterna av tekniken börjar synas. Ett annat särskilt tema som behandlades i prognosarbetet var cybersäkerheten och riskhanteringen i genomförandet av 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[1, 2], Cybersäkerhetscentrets webbplats.

I fråga om prognosarbetet fortsatte vi även att bygga upp samarbetet med olika aktörer. I takt med att verksamhetsmiljön förändras och kompliceras kommer samarbetets roll i identifieringen av framtida fenomen och deras olika effekter att bli ännu viktigare. Genom samarbete stöds delningen och utnyttjandet av information i all verksamhet.

Under 2022 fortsatte vi att utveckla tjänsterna HAVARO och Cybermätaren. HAVARO upptäcker allvarliga informationssäkerhetshot mot finländska företag och varnar om dem. Cybermätaren i sin tur är en nationell bedömningsmodell för cybersäkerheten som möjliggör kontinuerlig bedömning, utveckling och jämförelse av organisationernas cybersäkerhet mellan olika aktörer i en referensgrupp.

Under 2022 genomfördes flera cyberövningar. Inte ens goda verksamhetsmodeller och anvisningar är nödvändigtvis tillräckliga om man inte vet hur man ska använda dem när det verkligen gäller. Med hjälp av övning är det enkelt att implementera goda och korrekta processmallar i organisationens verksamhet, vilket klart har ökat intresset för cyberövningar. Under 2022 genomfördes också flera sektorsspecifika samövningar inom cybersäkerhet. Organisationerna ser sig själva tydligare som en del av ett större organisationsnätverk eller en större leveranskedja, och därför har man under den senaste tiden även upplevt att det är ännu viktigare än tidigare att öva på gemensamma processer. Cybersäkerhetscentret stöder cyberövningarna genom rådgivningstjänster och anvisningar samt genom att erbjuda idéer till scenarion som innehåll i övningarna och stödja planeringen och genomförandet av nationellt betydande samövningar.

[1] Artificiell intelligens kommer också att förändra cyberangreppen | Traficom (kyberturvallisuuskeskus.fi/sv)
[2] Information om cyberhot och riskhantering för lokala mobilnät i en ny anvisning | Cybersäkerhetscentret

Man försökte öka medvetenheten om cyberhot på många olika sätt

Under 2022 försökte man aktivt öka medvetenheten om cyberhot i Finland. Till exempel olika myndigheter, företag och organisationer informerade regelbundet om cyberhot samt utfärdade och publicerade anvisningar och varningar om det aktuella cybersäkerhetsläget, till exempel om observerade bedrägerimeddelanden.

I Cybersäkerhetscentrets olika kommunikationskanaler, till exempel på webbplatsen och i sociala medier, informerade vi aktivt om frågor i anknytning till centrets verksamhet, cyberhot och det aktuella säkerhetsläget. Under 2022 ordnades ett flertal evenemang, såsom cybersäkerhetsmärkes- och informationssäkerhetsseminarierna, som syftade till att öka det finländska informationssäkerhetssamfundets och ledningens kunskap om den kommande regleringen av cybersäkerheten och informationssäkerhetsområdet, om förändringarna i säkerhetsmiljön och om deras effekter på cybersäkerheten. Seminariet Informationssäkerhet, som ordnades i oktober tillsammans med Försörjningsberedskapscentralen, samlade över 1 000 deltagare. Huvudtalare vid evenemanget var Ukrainas biträdande minister för digital omvandling, George Dubynskyi.

År 2022 lanserades Cybersäkerhetscentrets nya veckoöversikt som behandlar aktuella cyberfenomen.

I översikten Cybervädret, som publicerades varje månad, berättades om betydande informationssäkerhetsincidenter och -fenomen under den gångna månaden. Produkten är i första hand avsedd för personer som är ansvariga för informationssäkerhet, men i avsnittet om cybersäkerhet i vardagen finns det goda råd för alla. Översikten ger snabbt en överblick över vad som har skett inom cybersäkerhetsområdet. Översikten Cybervädret förnyades i slutet av året. Produkten kommer framöver att rikta sig till organisationer och skapar tillsammans med Veckoöversikten en gemensam helhet så att aktuella teman lyfts fram i Veckoöversikten för snabb delning av informationen. Cybervädret i sin tur sammanfattar månadens händelser i korthet, men fokuserar på kort- och långsiktiga trender samt hot, som organisationerna rekommenderas att förbereda sig för.

Cyberhoten ändrar hela tiden form. Medvetenheten hos och förmågan för organisationer, sakkunniga på informationssäkerhetsområdet och den stora allmänheten att identifiera och svara på cyberhot samt förbättra den egna informationssäkerheten främjades genom att publicera flera guider och anvisningar på centrets webbplats. Exempel på guider och anvisningar som publicerades under 2022 var anvisningar om åtgärder vid angrepp med utpressningsprogram för ledningen, en översikt över läget i fråga om överbelastningsangrepp, anvisningar för situationer med läckta användarkoder, en översikt över tryggandet av energiförsörjningen i kommunikationsnäten samt en beskrivning av Finlands internationella dataförbindelser och beredskapen för hoten mot deras funktion. Dessutom publicerade vi tips för identifiering av informationspåverkan och anvisningar för användning av flerfaktorsautentisering för att skydda användarkonton.

Under 2022 genomförde eller deltog Cybersäkerhetscentret i ett flertal kommunikationskampanjer. Dessa var till exempel kampanjen Smarta inköp, som genomfördes i slutet av året och som syftade till att öka konsumenternas kunskap om informationssäkerhetsfrågor i anknytning till smarta enheter, och den europeiska cybersäkerhetsmånaden, som genomfördes i oktober. I sina tv-kanaler sände Rundradion dessutom på hösten som allmännyttig reklam en informationsvideo om hur man identifierar cyber- och informationspåverkan.

Centrets sakkunniga och ledning föreläste regelbundet på regionala och riksomfattande försvarskurser om teman kring cyberhot och beredskapen för dem. De sakkunniga gav även regelbundet intervjuer i finländska och utländska medier samt talade på seminarier och evenemang både i Finland och utomlands. Vi bedrev ett nära samarbete med högskolor och läroanstalter inom området. Med hjälp av en aktiv och öppen informationsdelning bidrog vi till spridningen av information och kompetens i samhället i fråga om cybersäkerhet.

Med hjälp av stödet för utveckling av informationssäkerheten påskyndas förbättringen av informationssäkerheten i företag som är kritiska för försörjningsberedskapen

I oktober 2022 fattade statsrådet beslut om ett tidsbegränsat stöd för utveckling av informationssäkerheten (den så kallade informationssäkerhetssedeln) för företag som är livsviktiga med tanke på samhällets funktion. Målet med stödet är att snabbt höja informationssäkerhetsnivån för företagen och därigenom förbättra hela samhällets förmåga att skydda sig mot cybersäkerhetshot. Cybersäkerhetscentret vid Transport- och kommunikationsverket ansvarar för beviljandet av stödet. För ansökan om och beviljande av stödet utvecklade man vid ämbetsverket i snabb takt system och processer som möjliggör ansökan om stödet, behandling av ansökningar och utbetalning av stödet elektroniskt. På så vis kan stöden så snabbt som möjligt beviljas de företag som ansökt om stödet.

Ansökan om informationssäkerhetssedeln öppnade i december, och redan under de första veckorna överskred eurobeloppet som söktes i ansökningarna om stöd anslaget på sex miljoner euro som statsrådet anvisat för beviljandet av stöden. Från och med början av 2023 kom behandlingen av ansökningar igång på allvar, och de första positiva besluten om stöd fattades i januari 2023. Efter att ha behandlat stödansökningarna har Cybersäkerhetscentret till uppgift att behandla utredningar om användningen av stödet som lämnas in av de företag som fått stödet. Samtidigt görs en bedömning av de åtgärder som genomförts och de fördelar som uppnåtts med hjälp av stödet.

> ”Målet med stödet är att snabbt höja informationssäkerhetsnivån för företagen och därigenom förbättra hela samhällets förmåga att skydda sig mot cybersäkerhetshot.

Cybersäkerhetsmärket beviljades för 15 nya enheter

Cybersäkerhetsmärket, som offentliggjordes av Cybersäkerhetscentret vid Transport- och kommunikationsverket Traficom år 2019, visar att en produkt eller tjänst som försetts med märket uppfyller Traficoms krav för en god grundnivå på 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 2022 beviljades 15 nya enheter Cybersäkerhetsmärket. För närvarande har sammanlagt 25 enheter beviljats märket. 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. Cybersäkerhetscentret vid Traficom förbereder sig för att ändra sin verksamhet för uppgifter i enlighet med regleringen ovan.

Cybersäkerhet

Förstärkning av forsknings- och utvecklingsverksamheten inom cybersäkerhet i Finland och Europa

Finlands nationella samordningscentrum inom ramen för Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning inledde officiellt sin verksamhet vid Cybersäkerhetscentret vid Transport- och kommunikationsverket i början av år 2023. Arbetet med att bereda Finlands nationella samordningscentrum inleddes hösten 2022. Samordningscentrumet stödjer finländska aktörers deltagande i gränsöverskridande EU-projekt och främjar öppnandet av möjligheter till EU-finansiering enligt nationella prioriteringar. Dessutom ordnar samordningscentrumet finansieringsansökningar för finländska aktörer för åtgärder som ökar cybersäkerheten.

Det nationella samordningscentrumet är en del av ett unionsomfattande nätverk av samordningscentrum inom ramarna för EU:s kompetenscentrum för cybersäkerhet. Nätverkets uppgift är att förbättra egenkapaciteten i cybermiljön, främja forskningen inom cybersäkerhetsområdet och sätta fart på den tekniska utvecklingen i hela EU. Med hjälp av nätverket som samordningscentrumen bildar ökar och intensifieras samarbetet mellan medlemsstaterna. I och med samarbetet stärks EU:s cybersäkerhetsberedskap och områdets konkurrenskraft. Samordningscentrumets verksamhet finansieras av EU och Finska staten.

Genom att utveckla regleringen främjas cybersäkerheten

Sörjandet för beredskapen och informationssäkerheten 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. Cybersäkerhetscentret vid Traficom styr och övervakar leverantörer av 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.

Cybersäkerhetscentret utfärdar föreskrifter som preciserar lagen för de aktörer som det övervakar. Föreskrifterna uppdateras regelbundet för att motsvara förändringarna i cybersäkerhetsmiljön och den tekniska utvecklingen. Ett exempel på detta är föreskriften om elektroniska identifieringstjänster och betrodda elektroniska tjänster som uppdaterades under 2022. Dessutom styr centret de aktörer som det övervakar genom att ge rekommendationer och anvisningar samt bistå dem vid tolkningen av lagstiftningen.

Cybersäkerhetscentret övervakar sitt verksamhetsområde ofta på olika sätt, till exempel genom att samla in anmälningar om störningar, fatta beslut om tillsyn och utföra inspektioner. Du kan läsa mer om centrets styrnings- och tillsynsverksamhet på vår webbplats: https://www.kyberturvallisuuskeskus.fi/sv/var-verksamhet/reglering-och-tillsyn

Under 2022 behandlade Cybersäkerhetscentret hundratals anmälningar om störningar och tiotals besvär om användningen av kakor på webbplatser. Centret gav dagligen råd om iakttagande av lagstiftningen och gav tiotals utlåtanden om till exempel förfrågningar om utveckling av lagstiftningen. Cybersäkerhetscentret hade ett kontinuerligt fungerande samarbete med de företag som det övervakar.

> ”Det nationella samordningscentrumet är en del av ett unionsomfattande nätverk av samordningscentrum inom ramarna för EU:s kompetenscentrum för cybersäkerhet.

Trender inom cyber-säkerheten år 2023

Under 2023 kommer hotnivån mot cybersäkerhetsmiljön högst sannolikt att fortsätta att vara hög och den tekniska utvecklingen fortsätta att vara snabb. Regleringen hårdnar och företagen är tvungna att följa den skärpta regleringen inom cybersäkerhetsområdet. Detta kräver resurser och tid. Samtidigt ligger ett hot om ekonomisk nedgång i luften, och det är brist på cyberexperter. Företagen måste skydda sin information och sina system mot de ökande cyberhoten och måste även göra betydande investeringar i cybersäkerheten. Därtill är företagen och organisationerna tvungna att lösa nya typer av cybersäkerhetsutmaningar, exempelvis bedrägeriförsök med hjälp av deepfake-videor samt bot-angrepp.

År 2023 försökte brottslingar utnyttja och ta i bruk ny teknik för att nå sina mål ännu effektivare än tidigare. Samtidigt som nya möjligheter och metoder för angrepp skapas till följd av att artificiell intelligens blir vanligare och alltmer en del av vardagen, erbjuder den även nya verktyg för att bekämpa dem. Till exempel chatbottar baserade på artificiell intelligens är ett effektivt redskap för bekämpning av bedrägerier och svindleri. Dessa bottar kan identifiera misstänkta meddelanden och varna användarna för eventuella bedrägerier. Det här är viktigt, eftersom bedragarna blir allt kreativare och kommer på nya sätt att komma över uppgifter och tillgångar.

Välutvecklade system för cyberförsvar, till exempel maskininlärning och dataanalys, kommer under de närmaste åren att bli allt viktigare med tanke på cybersäkerheten. Dessa system ger skydd i realtid och ett förebyggande skydd mot attacker mot informationssäkerheten. Det är nödvändigt, eftersom även bedragarna använder allt mer välutvecklad teknik och välutvecklade botsystem för att attackera informationssystem. Välutvecklade system för cyberförsvar ger ett viktigt skydd mot sådana angrepp.

Hur syns den höjda cyberhotnivån i vardagen?

Den höjda cyberhotnivån syns på flera olika sätt i den dagliga verksamheten för olika aktörer. De viktigaste utsikterna är:

Ökad informationssäkerhetsrisk: Företag och andra organisationer bör skydda sin information och sina system mot de ökande cyberhoten.

Skärpt reglering: Under de kommande åren kommer mer reglering inom cybersäkerhetsområdet att rikta sig mot företag och organisationer, vilket kommer att kräva resurser och kompetens.

Investeringar i cybersäkerhet: Företag och organisationer bör förbereda sig för att göra nya investeringar i cybersäkerhet för att de ska kunna skydda sin information och sina system.

Utmaningar som ny teknologi medför: Företag och organisationer blir tvungna att lösa nya typer av cybersäkerhetsutmaningar, exempelvis bekämpa deepfake-videor och botangrepp.

För att företagen och organisationerna ska kunna svara på dessa utmaningar, bör de göra följande ändringar:

Uppdatera sin informationssäkerhetsstrategi: Det behövs en aktuell informationssäkerhetsstrategi som svarar på de senaste cyberhoten.

Satsa på utbildning och personalen: Allt mer bör satsas på utbildning av personalen och dess kompetens i cybersäkerhet.

Sörja för regelbunden utvärdering av cyberhot och utveckling av den: Företag och andra organisationer bör se till att regelbundet utvärdera cyberhoten och vid behov utveckla sina system och processer.

Samarbete med partner: Det är möjligt att effektivisera cybersäkerheten i samarbete med partner och genom att utnyttja deras lösningar.

Hot om ekonomisk nedgång och brist på cyberexperter blir en utmaning

Företagens och andra organisationers förmåga att skaffa och upprätthålla nödvändiga cybersäkerhetsresurser till följd av de eventuella utmaningarna i ekonomin inom den närmaste framtiden blir en utmaning. Därför kan det hända att aktörerna prioriterar besparingar inom cybersäkerhetsområdet och låter bli att genomföra en del åtgärder. I företagen torde detta leda till exempelvis en ökad användning av utkontraktering och leveranskedjor samt i och med besparingsbehoven vidare att dessa minskas och prioriteras.

Bristen på cyberexperter försvårar företagens och andra organisationers förmåga att reagera och lösa cyberhot samt gör dem ännu mer mottagliga för angrepp. Därför är det viktigt för företag och organisationer att förbereda sig för och anpassa sig till dessa utmaningar genom att utveckla effektiva och flexibla lösningar samt skaffa och utbilda tillräckligt med kunniga personalresurser.

Upphandlingskompetensen i fråga om cybersäkerhet bör utvecklas kontinuerligt

Företag och andra organisationer bör kontinuerligt utveckla sin upphandlingskompetens i fråga om cybersäkerhet. Detta förutsätter till exempel en förmåga och kompetens i företagen att sammanjämka cybersäkerhetsbehov med affärsverksamhetens behov.

Köpta tjänster och leveranskedjor kan vara en betydande del av företagens lösningar för cybersäkerheten. De ger möjligheter att utkontraktera en del av ansvaren för cybersäkerheten samt utnyttja expertis och teknik som organisationen inte nödvändigtvis själv har.

När organisationer köper cybersäkerhetstjänster och cybersäkerhetsprodukter bör de säkerställa att tjänsterna och produkterna uppfyller de operativa och kvalitativa krav som ställs på dem. Detta förutsätter en förståelse av olika delområden av cybersäkerhet och de standarder, tekniker och tillvägagångssätt som är förknippade med dem. Dessutom behöver köparen kunskap om vilka tjänster och produkter som finns tillgängliga och om prisnivån och erbjudanden på marknaden samt förståelse om informationssäkerhets- och dataskyddsfrågor. Köparen bör även kunna bedöma serviceproducentens pålitlighet samt förmåga att erbjuda kontinuerligt stöd och uppdateringar.

Finns det bästa praxis för de informationssäkerhets- och dataskyddskrav som används vid upphandlingar som lätt kan tas i bruk? Ja, det finns det. Till exempel EU:s dataskyddsdirektiv och informationssäkerhetsregelverk, NIST Cybersecurity Framework samt informationssäkerhetsstandarderna ISO/IEC 27001 och 27002.

Lagstiftningen förändras – det är bra att vara proaktiv och förberedd

Det är bra för företag och andra organisationer att förbereda sig för att regleringen skärps och förändras. Det är nödvändigt, eftersom cyberangrepp blir allt vanligare och mer komplexa. Lagstiftningen bidrar till att skydda privat information och information i affärslivet samt förbättra den allmänna informationssäkerheten och funktionen. Det är möjligt att göra god informationssäkerhet till en konkurrensfördel.

EU-regleringen på cybersäkerhetsområdet kommer att öka. I februari 2022 kompletterades radioutrustningsdirektivet (RED) med obligatoriska informationssäkerhetskrav. I förordningen finns en övergångstid för tillverkarna, efter vilken trådlös utrustning som släpps ut på marknaden från och med den 1 augusti 2024 ska uppfylla kraven. NIS2-cybersäkerhetsförfattningarna för kritisk infrastruktur träder i kraft den 18 oktober 2024.

Det är bra för företagen att förbereda sig för EU:s cybersäkerhetsreglering på följande sätt under 2023:

- **Genomgång av författningarna och förberedelser för den nationella implementeringen av dem:** Företagen bör sätta sig in i den kommande regleringen, till exempel RED-direktivet och NIS2-cybersäkerhetsförfattningarna, och reda ut kraven i dessa som gäller dem själva.
- **Bedömning och riskhantering:** Företagen bör utvärdera sina nuvarande cybersäkerhetsnivåer och identifiera eventuella brister beträffande iakttagandet av kraven i regleringen.
- **Planering och genomförande av åtgärder:** Företagen bör planera och genomföra nödvändiga åtgärder för att iaktta kraven i regleringen, till exempel uppdatera informationssäkerhetsprogrammet och informationssäkerhetsprocesserna.
- **Utbildning för personalen och kommunikation:** Företagens personal bör vara medveten om regleringen och kraven i den. Personalen bör erbjudas nödvändig utbildning och information för att kunna iaktta regleringen.
- **Samarbete:** Företagen bör i samarbete med aktörer på området och eventuella stödtjänster förbereda sig för den kommande regleringen och effektivt iaktta den.

Hur kan vi stärka medborgarnas informationssäkerhetsfärdigheter även framöver?

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 bedrägerimeddelanden. Detta inkluderar även olika former av informationspåverkan, till exempel spridning av desinformation. Därför är det viktigt att man satsar på medborgarnas informationssäkerhetskompetens samt på att upprätthålla och utveckla deras medie- och teknikkunnighet.

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. Cybersäkerhetscentret stöder cyberfärdigheterna för medborgare på alla informationssäkerhetsnivåer.

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.

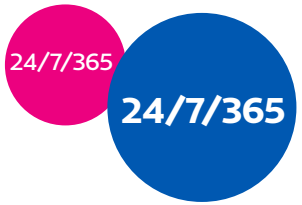
Aktiv, öppen och regelbunden kommunikation bidrar till att upprätthålla förtroendet. Man ska kommunicera öppet och transparent om såväl bra saker som problem.

I det digitaliserade samhället bör uppmärksamhet även ägnas åt att delaktigheten förverkligas. Hur får vi alla att hänga med i det digitala samhället? Hur säkerställer vi delaktigheten och deltagandet för olika befolkningsgrupper?

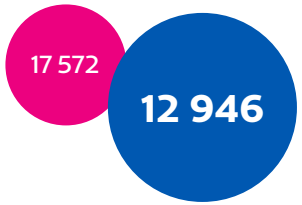
> ”Aktiv, öppen och regelbunden kommunikation bidrar till att upprätthålla förtroendet.

Nyckeltal för vår verksamhet

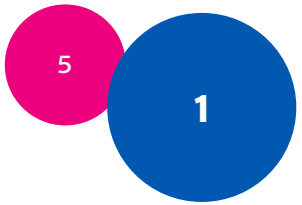
2021 2022



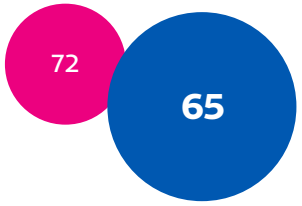
Oavbruten jour



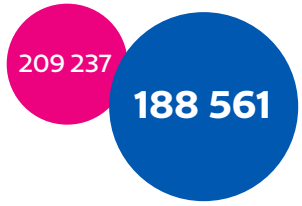
Behandlade fall



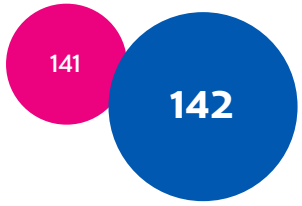
Varningar



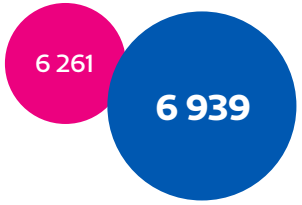
Fall som behandlats av sårbarhetskoordineringen



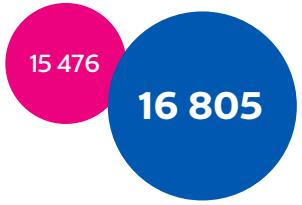
Autoreporter



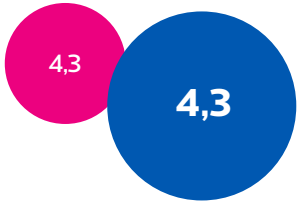
Kontakttillfällen från medier



Facebook-följare

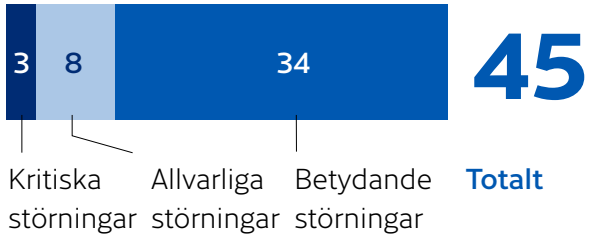


Twitter-följare (nu X)



Tillfredsställelse med lägesbildsprodukterna

Antalet störningar



Transport- och kommunikationsverket Traficom
Cybersäkerhetscentret
PB 320, 00059 TRAFICOM
tfn 029 534 5000

Kyberturvallisuuskeskus.fi/sv

Traficoms publikationer 16sv/2023
ISSN 2669-8757 (e-publikation)
ISBN 978-952-311-894-2

TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret