Transport- och kommunikationsverket
Cybersäkerhetscentret

Informationssäkerhet 2020

Cybersäkerhetscentrets årsöversikt

Traficoms publikationer

26/2021

Innehåll

Ledare 3

Cyberväderfenomen 4

- Nätens funktion 5
- Spionage och påverkan 9
- Skadlig programvara och sårbarheter 10
- Dataintrång och dataläckage 12
- Nätfiske och bedrägerier 14
- Föremålens internet och automationssystem 15

Våra tjänster 16

- Lägescentral – Första hjälpen vid informationssäkerhetskränkningar 17
- Behovet av sårbarhetskoordinering har ökat 18
- Säkerhetsreglering 19
- Bedömningar 21
- Satellitsystemen syns redan i människornas vardag 22
- Samarbete och informationsdelning 26
- Coronakrisen gjorde det internationella cybersäkerhet elektroniskt 28
- Övningar ger mer verksamhetssäkerhet 28
- Cybersäkerhetsmärket 29
- Den avgiftsfria Traficom Anycast-tjänsten förbättrar funktionssäkerheten hos .fi-domännamn 30
- Säkrare 5G med hjälp av lärdomar 31
- KYBER 2020 och den förnyade HAVARO-tjänsten 31
- Cybermätaren – Ett nytt verktyg för ledningen för att hantera cyberrisker 32

Nyckeltal för vår verksamhet 34

Cybervädret 2020 och blicken mot 2021 36

- 10 informationssäkerhetsutsikter för 2021 36
- Cybervädret 2020 38

Cybersäkerheten togs permanent med på ledningens agenda

Säkerheten i mobilnäten, särskilt 5G-näten, var ett av de mest omtalade ämnena i världen. EU utarbetade skyndsamt anvisningar om åtgärder för att minimera cybersäkerhetsriskerna i 5G-näten. I Finland förbereddes ny lagstiftning för att skydda kommunikationsnätens kritiska delar. I den nya lagstiftningen är den nationella synvinkeln mer betonad än tidigare, och den ger även nya verktyg att ingripa i eventuella cybersäkerhetsrisker som hotar den nationella säkerheten och försvaret.

Under det gångna året mötte vi på det hittills största dataintrånget i Finland då Psykoterapicentret Vastaamos patientuppgifter hamnade i händerna på brottslingar. Med de stulna uppgifterna utpressade angriparna både Vastaamo och tiotusentals medborgare som använt dess tjänster. Vi hjälpte offren bland annat med anvisningar samlade på webbplatsen tietovuotoapu.fi och tillsammans med myndigheter, organisationer och företag. Fallet Vastaamo väckte samhällelig debatt om företagsledningens ansvar för att skydda kritiska datalager och informationssystem. Det påminde oss även om att personbeteckningen inte passar som identifikationsmetod i nättjänster.

Året färgades även av den skadliga programvaran Emotet som vi publicerade en varning om i augusti. Syftet med den skadliga programvaran är att stjäla organisationens uppgifter. Med angreppet är det möjligt att tränga in djupt i objektets nät och inleda till exempel ett angrepp med utpressningsprogramvara. Emotet är ett bra exempel på ett professionellt genomfört dataintrång i syfte att få fotfäste och öppna en dörr till organisationen som råkar ut för intrånget.

I början av året flyttade pandemin oss i stora skaror hem för distansjobb. Därmed började även utnyttjandet av sårbarheterna i olika distansarbetslösningar öka inom dataintrången. Dessutom fattade internationella cybertrender greppet om Finlands telenät i februari då en våg av bedrägerisamtal svepte genom landet. Enbart under februari rapporterade finländska teleoperatörer miljontals bedrägerisamtal.

Men det tunga året medförde även något gott. Jouko Katainen (Ilmarinen), Jussi Törhönen (Enfo), Tomi Vehkasalo (Aditro) och Jani Räty (Aditro) fick utmärkelsen Vägvisare för informationssäkerheten för sitt aktiva samarbete med Cybersäkerhetscentret. Dessutom deltog vi i arbetet med att skapa applikationen Coronablinkern. Dess informationssäkerhets- och dataskyddslösningar verkar ha träffat rätt. Nu använder miljontals finländare applikationen och stöder hanteringen av coronasituationen i vårt land.

Undantagsåret visade även att det går att flytta arbetet till webben och uträtta ärenden via e-tjänster på ett säkert sätt. Vi såg även att vi i samarbete med myndigheter och medborgarorganisationer kan hjälpa till med mänskliga kriser orsakade av cyberbrottsligheten. Händelsernas allvar och konsekvenser lyfte permanent upp cybersäkerheten på ledningens agenda.

År 2021 firar vi tjugoårsjubileet för vår CERT-verksamhet. De här årtiondena har innehållit många överraskningar.

Följ vår webbplats och våra sociala medier! Om ni är intresserade av cyberprognoserna för 2021 kan ni hitta dem i slutet av översikten.

Helsingfors den 11 februari 2021,

Sauli Pahlman
Tf överdirektör
Cybersäkerhetscentret

Cybervädерfenomen

Nätens funktion

Störningar i kommunikationsnäten

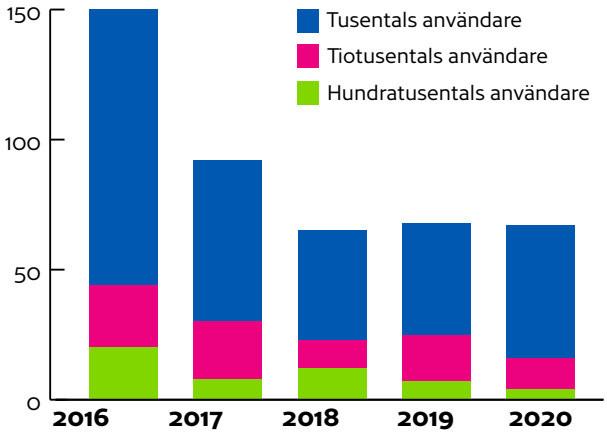
Det är viktigt att de inhemska kommunikationsnäten fungerar så pålitligt och störningsfritt som möjligt. Annars kan exempelvis de digitala tjänsterna i vårt samhälle inte fungera. Utifrån de störningsuppgifter vi samlat in kan vi analysera störningarnas grundorsaker och förbättra nätens funktionssäkerhet bland annat genom att utveckla regleringen.

Antalen betydande störningar minskade klart fram till 2018 och har sedan dess legat på mellan 65 och 68. År 2020 förekom 67 betydande störningar. Antalet kritiska störningar som gäller åtminstone 100 000 användare minskade dock. Som helhet kan utvecklingsriktningen anses vara positiv även om minskningen av betydande störningar har stannat upp.

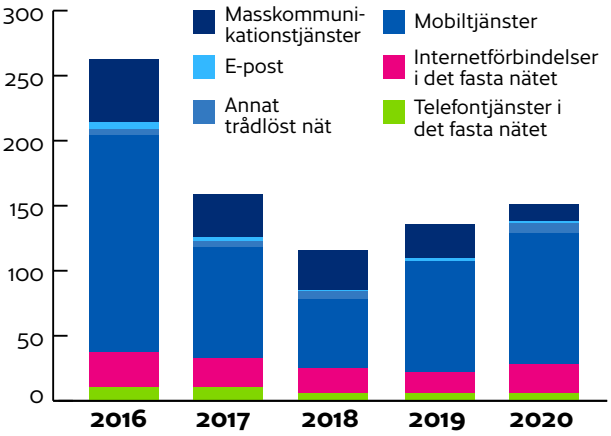
Majoriteten av de betydande störningarna i de inhemska kommunikationsnäten gäller tjänster i mobilnätet, funktionen hos samtal, internetförbindelser och textmeddelanden. De beror till exempel på elavbrott orsakade av stormar som även inverkar på eltillförseln till mobilnätets basstationer. Mobilnätet är även tekniskt mer komplicerat än till exempel det fasta bredbandsnätet och därför är bland annat störningar som beror på programfel vanligare i mobilnät.

Antalet störningar som beror på fel i motoranläggningssystem och programfel ökade från 2019. Noggrann testning av systemen kan minska på störningarna. Därför lönar det sig även att övervaka utrustning och programkomponenter, eftersom komponenter som fungerar opålitligt kan förbli dolda i testerna.

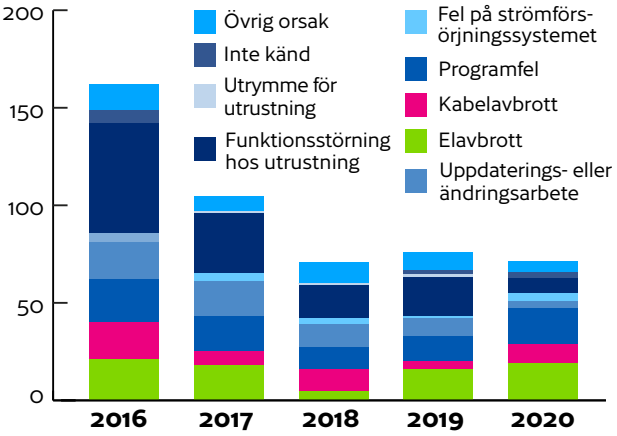
Uppdaterings- och ändringsarbetena däremot orsakade mindre störningar än tidigare. Detta är en god nyhet och vittnar om att telebolagen har arbetat långsiktigt för att utveckla underhållet av sina tjänster.



Antalet betydande funktionsstörningar i de allmänna kommunikationstjänsterna 2016–2020.



Konsekvenserna av betydande funktionsstörningar på allmänna kommunikationstjänster 2016–2020. En störning kan inverka på flera tjänster.

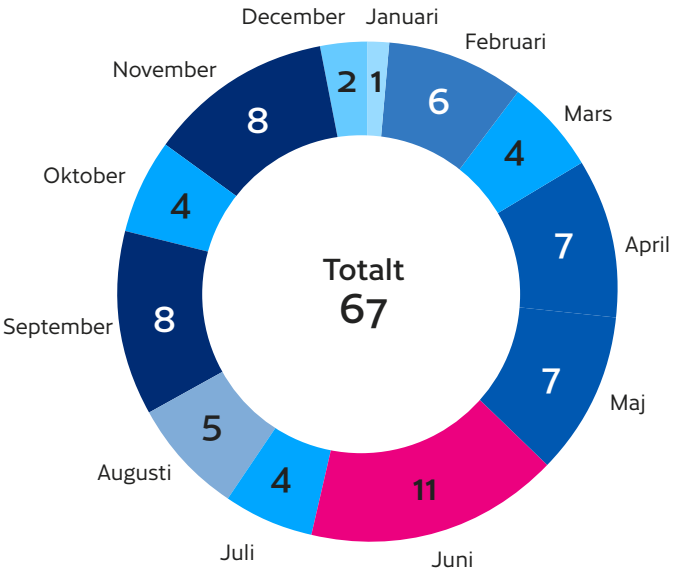


Grundorsaker till betydande funktionsstörningar 2016–2020. En störning kan ha flera grundorsaker.

Internetavbrott förekom runt om i Finland och stormarna orsakade elavbrott

Den nationella störningen i internetförbindelsetjänsten i Telias mobilnät den 25 april väckte även mediernas uppmärksamhet.

Även stormarna orsakade betydande funktionsstörningar. Våra kommunikationstjänster bröts särskilt av Päivö den 30 juni och Aila den 16–17 september. Telebolagen, elnätsentreprenörerna och räddningsverken skötte hanteringen av de funktionsstörningar dessa orsakade på rutin. Störningarnas konsekvenser förblev rätt små jämfört med stormarna för några år sedan.



Fördelningen av betydande funktionsstörningar på kalendermånaderna.

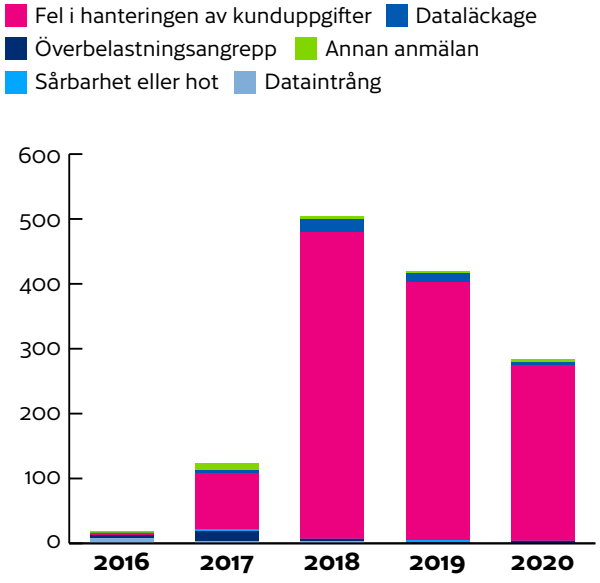
Distansverktygen väckte oro

De allmänna kommunikationstjänsterna höll väl i Finland och i övriga Europa även om människorna i stora skaror övergick till distansjobb då coronapandemin bredde ut sig.

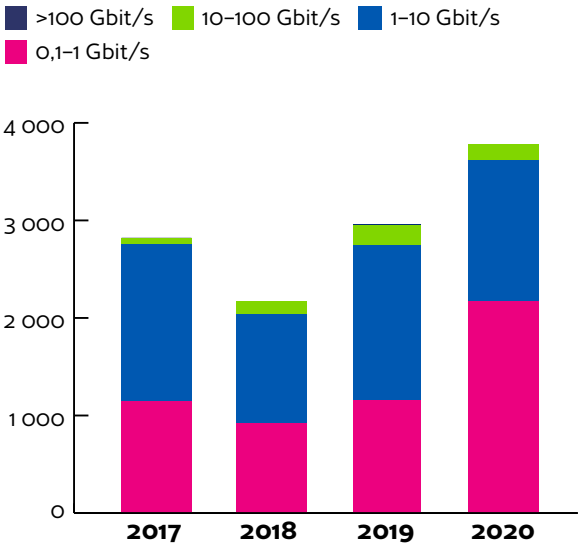
I början av pandemin förekom det kapacitetsproblem exempelvis i organisationernas egna VPN-tjänster och de internationella molntjänsterna. De löstes i regel på några veckor. I mars fler-dubblades användningen av molntjänster globalt. I flera organisationer tog man okontrollerat i bruk distansarbetsredskap och -tjänster, vilket kunde leda till ohanterliga informationssäkerhetsrisker.

Vi gav råd bland annat i användningen av split tunnel-tekniken. Med tekniken kan man exempelvis styra programmens uppdateringstrafik förbi VPN och därmed minska belastningen på organisationens VPN-tjänst.

Fel och bortglömda saker i behandlingen av webbtjänsternas certifikat orsakade omfattande störningar på användbarheten hos otaliga tjänster.



Telebolagens anmälningar om betydande informationssäkerhetskränkningar och informationssäkerhetskränkningar riktade mot personuppgifter 2016–2020.

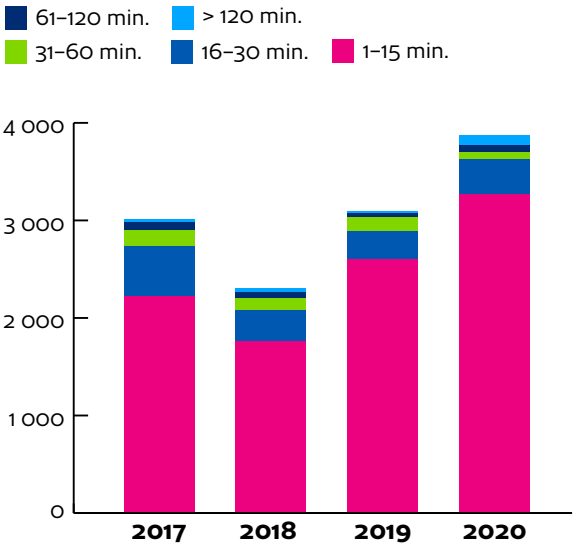


Utvecklingen hos överlastningsangreppens volym i Finland. Källa: Telia

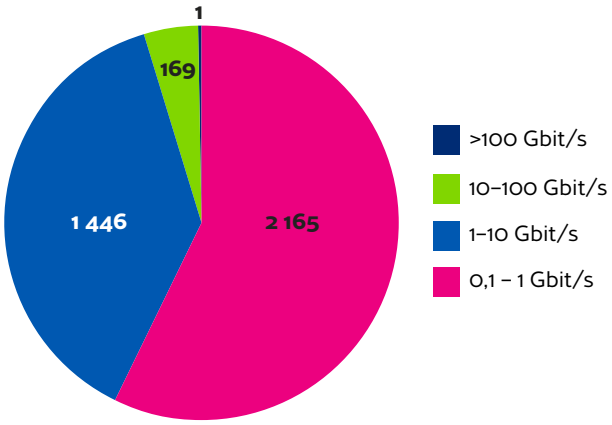
Microsoft Teams certifikat föråldrades i februari. Som tur är fick man läget under kontroll före pandemitiden, eftersom störningen kraftigast drabbade länderna i väst där Teams-tjänsten är vanlig. Let's Encrypt tvingades annullera beviljade certifikat i rask takt i början av mars och DigiCert gjorde likadant i juli eftersom det inträffat fel i behandlingen av deras begäran om certifikat. Det är viktigt att organisationerna har tydliga och snabba processer för att förnya certifikaten för sina webbtjänster.

Telebolagens anmälningar av informationssäkerhetskränkningar minskar alltjämt

Antalet anmälningar av telebolagen om informationssäkerhetskränkningar som gäller personuppgifter har minskat i jämn takt sedan toppen 2018. En typisk informationssäkerhetskränkning som gäller personuppgifterna är att telebolaget har antecknat fel adress för kunden och skickar ett brev eller e-postmeddelande till adressen med kundens personuppgifter. Det inträffar vanligtvis färre än tio betydande informationssäkerhetskränkningar. År 2020 anmäldes fem sådana.



Utvecklingen hos överlastningsangreppens längder i Finland. Källa: Telia



Fördelningen av överlastningsangreppens volymer i Finland 2020. Källa: Telia

Överbelastningsangrepp

De inhemska organisationerna har varje år förberett sig lite bättre på överlastningsangreppen. De filtreringstjänster som operatörerna erbjuder och organisationernas kompetens har blivit vanligare och bättre, vilket innebär att de vanligaste överlastningsangreppen just inte alls kan inverka på företagens verksamhet. Även överföringen av tjänsterna till molntjänsterna har förbättrat beredskapen inför överlastningsangreppen.

Under undantagsförhållandena betonas tillgången till nättjänster

I internationella nyheter kunde vi läsa om överlastningsangrepp som är stora till storleken och som exempelvis har inverkat på infrastrukturtjänster på internet. Man har år efter år förberett sig bättre inför angreppen, men ett långvarigt och stort angrepp kan ändå ha en omfattande inverkan på företagets verksamhet.

Under sommaren ökade antalet distansarbete på ett aldrig tidigare skådat sätt även i Finland. Överbelastningsangreppen har i vissa fall haft en indirekt inverkan på exempelvis organisationens interna tjänster såsom Skype och VPN-lösningar. De tjänster som är kritiska för distansarbetet bör planeras och genomföras så att överlastningsangreppen påverkar dem så lite som möjligt.

Även 2020 påträffades angrepp mot skolornas system. Det kan ha varit unga bakom angreppen, som inte förstår allvaret i överlastningsangrepp. Att göra eller försöka göra ett överlastningsangrepp kan tolkas som ett brott som kan leda till böter eller högst två års fängelse för gärningsmannen.

Vanligtvis får vi anmälningar om överlastningsangrepp i storleksklassen under 10 Gbit/s. Det största angreppet som anmäldes till oss i fjol var 161 Gbit/s.

Under hösten råkade europeiska operatörer ut för överlastningsangrepp. Angriparna hade särskilt siktat in sig på internets olika infrastrukturtjänster och särskilt DNS-servrar. Angreppen rapporterades ha nått en storlek på hela 300 Gbit/s och varat i flera timmar.

Ifjol såg vi även överlastningsangrepp i Europa som riktade sig mot digitala tjänster. Enligt serviceproducenterna var de överlastningsangrepp de märkt större än någonsin.

Överbelastningsangrepp användes för att utpressa företag även i Finland

Överbelastningsangrepp används även för att effektivera utpressningsprogrammens krav på lösen.

Ute i världen ökade utpressningsangreppen särskilt hösten 2020. I angreppets första skede får företaget ett e-postmeddelande där mottagaren pressas på oftast BitCoins för att angreppet inte ska genomföras. Ofta skickas utpressningsmeddelandet undertecknat av en känd kriminell grupp eller enskild aktör inom branschen. Oftast kryddar brottslingen sitt hotfulla meddelande med korta men kraftiga överlastningsangrepp för att försöka tvinga offret att betala pengar för att undvika större angrepp.

Vi känner till fall där man hotat med ett angrepp på upp till 2 Tb/s. Oftast har utpressningsmeddelandena varit oskäliga, men angriparen har kunnat utföra mindre överlastningsangrepp.

Även finländska organisationer anmälde till oss att de tagit emot utpressningsbrev. Enligt våra uppgifter genomfördes angreppen inte. Den penningsumma som krävdes var liten och utpressningsmeddelandena skickades av varierande källor. Organisationerna som utsattes för utpressningen hade inga förenande faktorer. Den som angrep verkade ha valt sitt mål slumpmässigt i hopp om pengar.

Vårt gamla råd har inte förändrats: betala inte åt en utpressare.

Spionage och påverkan

År 2020 verkade cyberspionagets tyngdpunkt ligga någon annanstans än i Finland, men även finländska organisationer var regelbundet utsatta för försök till intrång. Större nyheter om cyberspionagefall som lyckades har bland västländerna koncentrerats till de stora EU-länderna och USA med allierade.

Även EU och Norge tog under det avslutade året mer synligt ställning till krafterna bakom cyberangreppen och till exempel EU utfärdade sanktioner kring dessa.

Pandemin avspeglades även i cyberspionaget

I början av året avslöjades sårbarheter i lösningar som används för att trygga informationsnätens säkerhet och säkra förbindelser. Dessa sårbarheter utnyttjades eventuellt även i de cyberangrepp som statliga aktörer utförde. Oron kring årsskiftet gällde särskilt sårbarheter som upptäckts i vissa Citrix-produkter. Under året hittades även motsvarande sårbarheter i flera andra tillverkares produkter för informationsnät och för att trygga nätet.

I samband med vårens viruspandemi blev särskilt följande teman intressanta perspektiv:

1. Utnyttjandet av informationsspridningen kring coronaviruset och av olika rädslor i nätfiskemeddelandena eller i spridningen av skadlig programvara

2. Cyberspionage riktat mot coronaviruset, vården av det och vaccinforskningen.

Vi informerade organisationerna direkt om eventuella hot via våra kontakter, samarbetsnätverk och partner.

”Även om cyberspionaget främst riktade sig utanför Finland var även inhemska organisationer föremål för intrångsförsök.

Flera betydande dataintrångsfall i slutet av året

På hösten hade vi mycket arbete med fall av cyberspionage. Till exempel berättade Europeiska läkemedelsmyndigheten (EMA) att de råkat ut för dataintrång just innan det var tänkt att ett coronavirusvaccin skulle godkännas av verket. Redan tidigare på hösten lyfte Norge fram ett dataintrång riktat mot landets parlament Stortinget. Offentligt misstänkte de att APT28 som kopplas till den ryska militära underrättelsetjänsten (GU, tidigare GRU) låg bakom intrånget.

Finlands riksdag berättade å sin del i slutet av december om ett cyberangrepp riktat mot riksdagen. Centralkriminalpolisen undersökte det som grovt dataintrång och spionage. Riksdagen berättade att en del e-postkonton – bland dem även riksdagsledamöters konton – äventyrades under ett angrepp under hösten.

I slutet av året konkretiserades åter hot kring underleverans- och leveranskedjor då ett dataintrång riktat mot flera amerikanska ministerier och organisationer avslöjades. Dataintrånget var kopplat till distanshanteringsprodukterna SolarWinds. Angriparen hade lyckats smyga in sin kod i den uppdatering som delades ut till kunderna. På så sätt hade angriparen tillgång till alla organisationer som hade installerat uppdateringen med den skadliga koden. Det fanns sådana organisationer även i Finland. Enligt rådande uppfattning utnyttjade angriparen dock inträdesmöjligheterna endast till få utvalda objekt i andra länder än Finland.

Traditionella metoder används ännu

Även traditionella intrångsmetoder som att exempelvis maskinellt gissa lösenord och riktat nätfiske är en del av cyberspionagets metoder. Till exempel märktes många försök att knäcka lösenord under året.

Statliga cyberrisker riktade mot kritisk industriproduktion, logistik och energiförsörjning förekom också, främst i Mellanöstern.

Beredskapen för cyberspionage bör förbättras

Även om organisationernas iakttagelseförmåga och beredskap förbättrades ytterligare, finns det ännu brister till exempel i omfattningen på insamlingen av loggar och i hanteringen och analyseringen av dessa. Detta försvagar de finländska organisationernas förmåga att utreda dataintrång eller försök till dataintrång riktade mot dem. Ännu i dagsläget kan en stor del av dataintrången bara delvis utredas. Det är vanligt att man i utredningen inte når en säkerhet som tillfredsställer alla parter om hur händelseförloppet gick och vilka följder det hade.

Cyberspionage gäller inte bara statsförvaltningen eller politiska organisationer utan kan även riktas mot företag som exempelvis industrispionage. I beredskapen är det även bra att beakta riktade cyberangrepp som beställaren köper av kunniga aktörer. Beställningsangreppen försvårar även beredskapen för angrepp och identifieringen av aktörerna.

Skadlig programvara och sårbarheter

Under det gångna året såg vi vågor av sårbarheter och spridning av skadlig programvara som krävde snabba reaktioner. Även i distansarbetslösningarna hittades stora sårbarheter som utan dröjsmål behövde uppdateras eller åtminstone beaktas i olika genomföranden.

Utvärdera distansarbetslösningarna ur informationssäkerhetssynvinkeln

I april hittade vi flera RDP-tjänster som var öppna för internet. Vi meddelade administratörerna om våra observationer och rekommenderade åtgärder. Sårbarheterna som hittades i distansarbetslösningarna användes för dataintrång, för att sprida skadlig programvara och använda utpressningsprogram.

Överlag erbjöd fjolåret angriparna flera möjligheter att tränga in i organisationernas nätmiljöer. Även informationssäkerhetsluckorna i de mer vanliga distansarbetslösningarna och fildelningstjänsterna erbjöd möjligheter till detta.

Nätangreppens så kallade angreppsyta ökas betydligt av de tjänster och deras sårbarheter som syns i det offentliga nätet eller finns tillgängliga för angriparen. Genom att skydda oss, avgränsa tjänsternas synlighet eller ta onödiga tjänster ur bruk minskar vi på de metoder angriparen har tillgång till för att tränga sig in i nätet.

> ”Genom att skydda oss, avgränsa tjänsternas synlighet eller ta onödiga tjänster ur bruk minskar vi på de metoder angriparen har tillgång till för att tränga sig in i nätet.

Efter att angriparen tagit sig in i det interna nätverket kan hen gissa lösenord och utnyttja andra sårbarheter som inte har lappats med uppdateringar. Distansarbetsarrangemangen skulle inte få äventyra en enda organisations informationssäkerhet. Undantagslösningar, om sådana används, borde hävas då vi återgår till det normala. Utan dokumentering av lösningarna går det inte att häva dem omsorgsfullt.

Uppdateringar kan vara räddningen mot stora skador

Då en sårbarhet blir känd skannas den aktivt genast efter publikationen. Om man dröjer med att installera uppdateringarna bör man kontrollera att en angripare inte redan hunnit utnyttja sårbarheten.

Innan man köper en ny maskin ska man alltid kontrollera om det även i framtiden finns uppdateringar för maskinens programvara. Om uppdateringarna upphör är operativsystemen mer utsatta för dataintrång. Även i Finland används flera gamla Windows-versioner som inte längre uppdateras även fastän det gäller kritiska sårbarheter.

Emotet spreds och utpressningsprogrammen ökade

I augusti publicerade vi en varning om en skadlig programvara vid namn Emotet som aktivt spreds i Finland. Emotet spreds exempelvis via bilagornas makro och skadliga länkar. Det försökte spridas med bedrägerimeddelanden som skickades som fortsättning på en gammal e-postkedja. Länkar och filer i e-postmeddelanden och förfalskade avsändaruppgifter är viktiga i smittorna med skadlig programvara. Organisationen borde fästa uppmärksamhet vid hur man behandlar förfalskade avsändaruppgifter i sin e-post.

Man bör även i Finland förbereda sig på hotet med utpressningsprogram eftersom de allt mer vanliga angreppen kan riktas mot organisationer av alla storlekar. Det är typiskt för utpressningsprogram att de aktiveras under veckoslut eller sådana tidpunkter då det är färre anställda på plats. Företagens betalningsberedskap eller -vilja har minskat och därför utvecklar brottslingarna nya sätt att utnyttja och sälja den information de kommit över. Ifjol blev trenden där brottslingarna inte bara krypterade informationen utan stal uppgifter från offret och hotade med att publicera dem om lösen inte betalas ut allt vanligare.

> ”Man bör även i Finland förbereda sig på hotet rån utpressningsprogram eftersom de blir allt vanligare och kan riktas mot organisationer av alla storlekar.

Vår uppskattning av de största sårbarheterna 2020

1. **VPN:** många olika sårbarheter och flera tillverkare – problem med alla.
2. **Zerologon:** en aktivt utnyttjad protokollsårbarhet.
3. **SMBGhost/SMBleed:** kritiska protokollsårbarheter.
4. **Oracle WebLogic:** en aktivt utnyttjad sårbarhet som möjliggör tillgången till servern.
5. **TCP/IP Treck / Ripple:** en global inverkan på hundra miljoner maskiner.

Alla sårbarheter har utnyttjats i dataintrång och de har använts av flera tjänster, gått att utnyttja på distans och varit synliga i det öppna nätet.

Dataintrång och dataläckage

Anmälningarna om dataintrång och dataläckage samt försök till sådana ökade. Det framkom just inga dataintrång riktade mot kommunsektorn som under 2019, men dataintrånget mot riksdagen blev offentligt i december.

I oktober rapporterades omfattande om psykoterapicentret Vastaamo som utpressades med hot om dataläckage. Det var frågan om det första dataintrånget i stor skala i Finland. Angriparen beslutade verkställa sitt hot delvis och läckte ut mycket sensitivt material i offentligheten.

Office 365-dataintrången och försöken fortsatte även 2020. Det verkar som om antalet fall inte håller på att minska markant.

I januari blev samtal från bedragare som utger sig för att erbjuda teknisk support vanliga. De följdes även upp av dataintrång där den som ringde upp uppmanade sitt offer att installera ett distansåtkomstprogram på datorn, som gav brottslingen tillträde till datorns uppgifter. I mars upphörde samtalen tillfälligt då mötesbegränsningarna till följd av den internationella pandemin trädde i kraft.

Den egna observationsförmågan skyddar mot brottslingar

Brottslingarna kartlägger ständigt nya möjligheter till angrepp, och därför spelar organisationernas egen observationsförmåga en viktig roll i skyddet mot angreppen. I nyckelposition står förmågan att observera händelser som avviker från det normala, exempelvis inloggningar en märklig tid eller från en märklig plats. Man bör även fästa uppmärksamhet vid loggningens kvalitet, kvantitet och tillräckliga förvaringstid, eftersom händelserna inte kan undersökas utan logguppgifter av hög kvalitet.

Via rapporterade meddelanden med skadliga program och nätfiske avslöjas ofta även dataintrång, och därför är alla anmälningar om informationssäkerhet viktiga för att skapa en lägesbild.

FALLET VASTAAMO

Dataintrånget mot Psykoterapicentret Vastaamo var det gångna årets största informationssäkerhetskränkning i Finland. Dataintrånget följdes av utpressningsmeddelanden där både Vastaamo och dess klienter krävdes på lösensummor om de ville undvika att deras patientuppgifter läcker ut på internet och blir tillgängliga.

Polisen har registrerat fler än 25 000 brottsanmälningar i fallet. Även många andra organisationer och myndigheter har deltagit och gett sitt stöd och sin hjälp till offren för dataintrånget.

Cybersäkerhetscentret undersökte behandlingen av fallet Vastaamo i början. Vi hjälpte även polisen och det informationssäkerhetsbolag som undersökte fallet med den tekniska utredningen.

Lärdomarna var uppenbara: man ska känna sina tjänster och hålla dem under uppsikt och utvärdera dem kontinuerligt. Om de egna resurserna eller kompetensen inte räcker till ska man be branschens proffs om hjälp. Att skanna webbtjänsterna och testa de egna systemen i cyberövningssyfte är en liten satsning jämfört med ett allvarligt dataintrång.

Fallet påminde oss även om att inte använda personbeteckningar för att identifiera kunder i nättjänster. En stark elektronisk identifiering är säkrare.

Mångsidigt och osjälviskt samarbete ger hjälp snabbt

Dataintrånget mot Vastaamo tog en ny vändning på lördagkväll den 24 oktober då brottslingen började utpressa Vastaamos kunder genom att hota med att publicera deras konfidentiella uppgifter.

Vi på Cybersäkerhetscentret började jobba på lördagskvällen. På söndag samlade vi flera olika myndigheter, organisationer och frivilliga för att sammanställa anvisningar för de som råkat ut för utpressningen. Till följd av arbetet publicerade vi måndagen den 26 oktober webbplatsen tietovuotoapu.fi för de som behöver hjälp. På sidan satte vi ut mångsidiga anvisningar av olika aktörer och kontaktinformation där offren även kunde få samtalshjälp.

Webbplatsen tietovuotoapu.fi visade hur fungerande, enkelt och vid behov snabbt samarbetet mellan olika organisationer är i Finland. Det var fint att vara med och bevittna hur alla ville skapa gemensamt väl trots sina sektors- eller ansvarsgränser. Det är lätt att bygga upp ett säkrare framtida samhälle på en sådan här tillit och samarbetsförmåga.

”Dataintrånget mot Vastaamo var den största informationssäkerhetskränkningen i Finland 2020.

Nätfiske och bedrägerier

Telefonbedrägerier gjorde undantagsåret mörkare

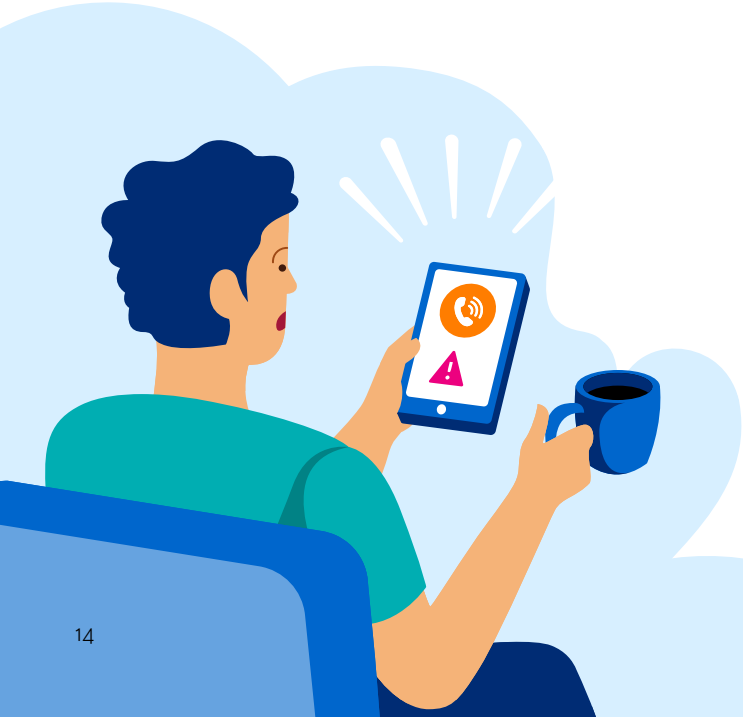
I februari hittade bedragarna verkligen Finlands telenät. Tidigare var antalet bedrägerier per telefon få i Finland.

Enbart under februari berättade finländska teleoperatörer om miljontals bedrägerisamtal från bedragare som utgav sig för att erbjuda teknisk support. Även de så kallade uppringningsbedrägerierna uppgick till en miljon samtal.

I bedrägerier med falsk teknisk support ringer bedragaren och berättar att det är ett problem på offrets dator. Bedragaren kan påstå att problemet beror till exempel på skadlig programvara, en hacker eller en ”internetstockning”. Vid uppringningsbedrägerier ringer offrets telefon en eller ett par gånger så att personen inte hinner svara. Samtalet kommer från ett utländskt riktnummer – Samoa, Papua-Nya-Guinea, Tunisien – eller från en satellittelefontjänst. Det kan kosta upp till 10 euro per minut att ringa upp numret.

Bedrägerisamtalen har orsakat mycket gråa hår och stora förluster för finländarna. Vårt samarbete med de finländska teleoperatörerna har hjälpt och vi har kunnat minimera uppringningssamtalen till Finland från utlandet. Efter juli har vi endast fått en handfull anmälningar om samtalen.

Det är svårare att bli av med bedrägerier med falsk teknisk support eftersom de telefonnummer bedragarna använder är förfalskade. Samtalen ser ut att komma från finländska, brittiska eller svenska telefonnummer, men i själva verket kommer de från en telefoncentral där tiotals anställda fabricerar bedrägerier på löpande band till olika länder.



Fakturabedrägerierna ger monetära förluster som känns

Fakturabedrägerierna orsakade återigen betydande ekonomiska förluster för organisationerna. Bland annat uppträdde en internationell kriminell grupp i Finansinspektionens och advokatbyråers namn för att nå penningtransaktionerna vid stora företagsförvärv.

Det vanligaste sättet att utföra ett faktureringsbedrägeri är att ge sig ut för att vara organisationens direktör och i dennes namn skicka meddelanden till organisationens ekonomipersonal. Engångsnyttan med brottet kan vara flera hundratusentals euro. Ofta märker man fakturabedrägerierna flera veckor i efterhand vilket gör det betydligt svårare att få tillbaka pengarna.

Bedrägerilänkar i textmeddelanden orsakade åter bekymmer

Länkar i textmeddelandena ledde ofta till prenumerationsfällor, skadliga program eller andra bedrägerier. Bedragarna använde ofta den här metoden. Den falska länkens adress syns nödvändigtvis inte på smarttelefonens ruta och därför kan mottagaren inte misstänka ett bedrägeri.

Särskilt i Postis och olika kurirfirmors namn skickades bedrägerimeddelanden ut. Syftet var att smitta Android-telefonerna med skadliga program och styra Apple-användarna till nätfiskesidor. Man ska inte tillåta installation av obekanta program på telefonen. Om man ger tillstånd kan ett skadligt program som skickar tusentals textmeddelanden utomlands orsaka abonnemanget stora räkningar.

Föremålens internet och automationssystem

Angrepp mot den kritiska infrastrukturens automationssystem

Det gångna året medförde angrepp mot den kritiska infrastrukturens automationssystem då angriparna tog sikte mot Israels vattensystem. Det första angreppet inträffade i april och i juni upptäcktes två nya försök. Israel lyckades förhindra angreppet som hade kunnat skada befolkningen på ett märkbart sätt.

Detta var veterligen första gången man med hjälp av IoT- och automationssystem försökte orsaka fysisk skada för en befolkning. Tidigare har angreppen främst riktats mot information och informationssystem. Iran misstänktes ligga bakom attacken. Angreppet anses vara det första tecknet på att cyberkrigföringen accelererar.

Tusentals maskiner och system har ännu inte skyddats

En undersökning om sårbarheten hos printrar från september visar att det alltjämt finns många informationssäkerhetsbrister i de smarta enheter som kopplats upp till nätet. Undersökningen hittade cirka 500 000 oskyddade printrar i nätet och valde att undersöka 50 000 närmare. Av dessa kunde hälften tas i besittning så att angriparen kunde printa ut med maskinen.

I vår årliga kartläggning av oskyddade automationsenheter gick vi i genom cirka 1 280 nät och 12,8 miljoner IP-adresser i den finländska cyberrymden. Vi hittade flest olika byggnadsautomationsenheter, som hade cirka 800 IP-adresser. Cirka 120 system inom industriautomationen och cirka 30 system inom den kritiska industriautomationen upptäcktes också. I de finländska näten hittade vi cirka 1 000 oskyddade automationssystem.

Jämfört med kartläggningarna de senaste åren har antalen inte förändrats markant och därför ska man fortsätta och effektivera informationssäkerhetsarbetet med maskinerna och systemen. Ju fler enheter med informationssäkerhetsbrister som förs ut på nätet, desto mer lider nätets användbarhet och informationssäkerhet.

> ”Ju fler enheter med informationssäkerhets-brister som förs ut på nätet, desto mer lider nätets användbarhet och informationssäkerhet.

En maskin utan skydd ute på internet är ett lockande föremål för inbrott. Maskinen kan användas till exempel för överbelastningsangrepp eller så kan den erbjuda lätt tillträde till företagets nät.

En märkbar förändring i IoT-världen i horisonten

Informationssäkerhetsproblem i IoT-enheter och automationssystem har fått många att lägga märke till behovet av de olika informationssäkerhetskraven och -certifikaten.

I EU:s cybersäkerhetsförordning som trädde ikraft i juni 2019 fastställdes ett certifikatsystem för den europeiska informationssäkerheten utifrån vilket man de kommande åren även planerar certifiering av IoT-enheterna.

I juni 2020 publicerades den första officiella informationssäkerhetsstandarden för konsumenternas smarta enheter ETSI 303645 Cyber Security for Consumer Internet of Things: Baseline Requirements.

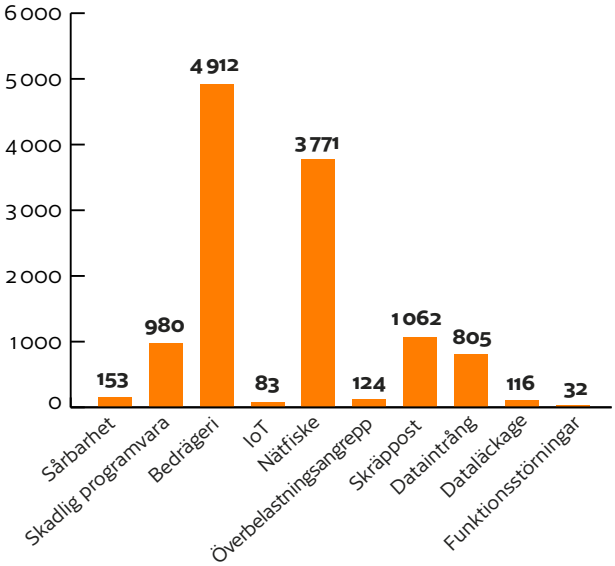
Även kommissionen märkte att informationssäkerheten hos enheter som kopplas upp på nätet ska förbättras även genom lagstiftning. En metod är EU:s direktiv om radioutrustning (Radio Equipment Directive, RED). Under det har man börjat förbereda en delegerad förordning om informationssäkerhet hos radioutrustning. Bestämmelsen kommer att ha en betydande inverkan på IoT-världen.

Våra tjänster

Lägescentral – Första hjälpen vid informationssäkerhetskränkningar

Informationssäkerhetsexperterna vid vår lägescentral ger första hjälpen och råd åt de som råkat ut för informationssäkerhetskränkningar. Antalet fall som vår central behandlade ökade med mer än 100 procent från 2019. Då var antalet fall 4 500 medan siffran 2020 var mer än 10 900.

Antalet fall ökade i praktiken i alla kategorier där vi klassar informationssäkerhetsincidenter. Vi fick flest anmälningar om olika bedrägerier och nätfiske.



Antalet fall per typ 2020.

Otaliga kontakter om den skadliga programvaran Emotet

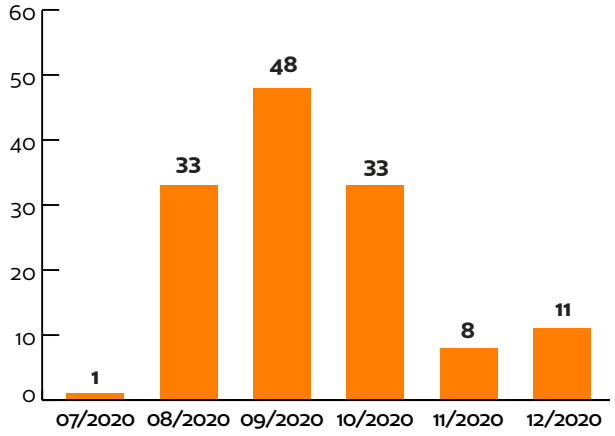
Emotet är ett bra exempel på en skadlig programvara i syfte att få fotfäste och öppna en dörr till organisationen som råkar ut för intrånget. Det används av brottslingar som utför professionella dataintrång. Vi fick de första anmälningarna om försöken att sprida den skadliga programvaran Emotet i augusti 2020.

En stor del av Emotet-fallen förblev endast spridningsförsök tack vare organisationernas egna informationssäkerhetskontroller. För andra gick det sämre. I smittofall gav våra jourhavande råd till flera offerorganisationer om hur de kan återhämta sig.

Vi publicerade den 18 augusti 2020 en gul varning om en aktiv spridning av den skadliga programvaran Emotet i Finland. Vi avlägsnade varningen i november även om det skadliga programmets hot inte helt vikit undan. Vi fick goda nyheter i januari 2021 då Emotet-botnätet kuvades genom en internationell polisoperation.

Då en kampanj som sprider skadliga programvaror hamnar i Finland vidtar vår lägescentral omedelbart åtgärder. Vi gräver fram de väsentliga detaljerna från kampanjen. Genom att dela informationsuppgifterna om så kallade skadliga program på våra olika kanaler erbjuder vi hjälp för att skydda sig mot hotet.

För att avvärja angrepp med skadlig programvara bör organisationerna skydda sig mångsidigt, till exempel genom att utbilda personalen och bygga upp tekniska kontroller.



Anmälningar om den skadliga programvaran Emotet per månad.

Identifikationsuppgift – Indicator of Compromise, IOC

- Till exempel IP-adress, domän eller url som det skadliga programmet använder som kommandokanal.
- Har din organisation förmågan att i loggarna leta efter trafik utifrån identifikationsuppgiften exempelvis för det senaste året?

Behovet av sårbarhetskoordinering har ökat

Lägescentralen får varje vecka meddelanden om sårbarhetsfall som kräver koordinering mellan produkten och komponenttillverkarna, informationssäkerhetsforskarna och användargrupperna. Största delen av fallen har en rätt enkel karaktär och de gäller nättjänster eller IoT-enheter.

Anmälningar om nättjänster är i huvudsak genomföringsfel i enskilda tjänster eller deras bakgrundssystem. I sådana här fall kan serviceproducenterna eller de underleverantörer som skapat koden själva reparera sårbarheten. Därför har de fall som rapporterats till oss inte kunnat orsaka några skador oss veterligen. År 2020 fick vi även fler anmälningar än året innan om dataskyddsbrister i tjänster och om misstankar kring brister.

> ”Ansvariga tillverkare reparerar oftast sårbarheterna snabbt och de öppna systemen uppdateras i bästa fall utan dröjsmål. Men det totala antalet öppna och riskabla tjänster verkar inte minska.

Nästan alla sårbarheter som rapporterades om IoT-enheter var till sin karaktär elementära fel på genomföringsnivån eller osäkra standardinställningar. I de flesta fallen kunde angriparen få kontroll över enheten med hjälp av sårbarheten. Processerna för att reparera sårbarheterna är ibland krångliga och långsamma.

Vi får ofta kännedom om öppna tjänster på internet som används för att säkerställa säkerheten eller hantera olika system. Behovet av öppenhet verkar ofta tvivelaktigt. Det riktas mycket angreppstrafik mot öppna tjänster och en enda svaghet eller felaktig inställning kan göra dem utsatta för dataintrång.

De allvarligaste sårbarheterna ifjol gällde fall där man hittade en ny sårbarhet i en tjänst som det finns flera av på nätet. Av en eller annan orsak var tjänsterna även öppna på nätet. Ansvariga tillverkare reparerar oftast sårbarheterna snabbt och de öppna systemen uppdateras i bästa fall utan dröjsmål, men det totala antalet öppna och riskabla tjänster verkar inte minska.

Säkerhetsreglering

Den nationella säkerheten tränger djupare in i kommunikationsnäten

Säkerheten i mobilnäten och framför allt 5G-näten var ett av de heta samtalsämnena runt om i världen under hela året.

Inom EU utarbetade man snabbt en politiskt neutral anvisning för åtgärder för att minska cybersäkerhetsriskerna i 5G-näten. I Finland förbereddes ny lagstiftning för att skydda kommunikationsnätens kritiska delar. Båda är tydligt närvarande i vårt arbete med att utarbeta anvisningar på EU-nivå och bereda en föreskrift om kommunikationsnätens kritiska delar för en ny lagstiftning. Tidigare hade man inte definierat de centrala delarna i kommunikationsnäten som används för att hantera och styra trafiken.

Redan i årtionden har den nationella säkerheten och försvaret varit en synvinkel i regleringen av kommunikationsnätens och -tjänsternas säkerhet. I den nya lagstiftningen är den nationella synvinkeln mer betonad än tidigare, och den ger även nya verktyg att ingripa i eventuella cybersäkerhetsrisker som hotar den nationella säkerheten och försvaret.

Positionsdatatjänst – webbinfrastrukturens nya hem

I oktober 2022 har vi finländare tillgång till Positionsdatatjänsten. Då kan den som ska börja utföra markbyggnadsarbeten få information om kablar och rör i grävområdet samt om var infrastruktur för tele-, el- och vattennät ligger. Syftet med tjänsten är att underlätta och effektivera planerarnas och markbyggarnas arbete. Den minskar även på kostnaderna och serviceavbrotten för tele-, el- och vattenbolagen och de som använder tjänsterna till följd av grävskador.

En centraliserad informationspunkt förbättrar nätverksaktörernas kännedom om var andra aktörers fysiska nätverksinfrastruktur ligger vilket underlättar samarbetet mellan dem. Enligt vår föreskrift (71/2020 M) ska uppgifterna som lämnas in till Positionsdatatjänsten ha en viss form vilket underlättar och förbättrar deras användbarhet. Föreskriften har även underlättat den tekniska specificeringen av funktionerna och de tekniska gränssnitten hos Positionsdatatjänsten.

Det är ännu långt tills vi kan ta Positionsdatatjänsten i bruk, men genom samarbete med olika sektorers representanter, aktörer som representerar markbyggnadsaktörer och Suomen Infratieto Oy kan vi nå vårt mål.

Pandemin visade att EU:s eIDAS-förordning behöver förnyas

Under undantagstiden ökade behovet av att uträtta ärenden och förhandla på distans och ingå avtal elektroniskt explosionsartat. Därför blev det även aktuellt med att utvärdera behovet av att förändra EU:s eIDAS-förordning.

Utifrån förordningen kan serviceproducenter skaffa godkännande på EU-nivå för sina förtroendetjänster som behövs i förvaltningen och affärsverksamheten till exempel för att göra avtal och tjänster elektroniska. Förordningen gäller inte bara informationssäkerhet utan även juridisk behörighet.

Vi väckte en inhemsk debatt om ändringsbehoven och samlade i juni erfarenheterna från det internationella och inhemska arbetet till en utvärderingspromemoria.

I Finland är den starka elektroniska identifikationen en etablerad och bekant tjänst, men man utnyttjar elektroniska signaturer och andra elektroniska förtroendetjänster i betydligt mindre grad. Vi fick rätt berömlig respons från sektorn om våra observationer.

I omvärderingen av eIDAS-förordningen bör man precisera kraven och lägga till tjänsteutbudet. Detta för att säkerställa en enhetlig reglering i de olika medlemsstaterna och förbättra förutsättningarna för utbudet. Ett ökat utbud av förtroendetjänster som besvarar kundernas behov underlättar i sin tur anskaffningen av dessa. Det råder till exempel mycket osäkerhet kring valet och ibruktagandet av elektroniska signaturtjänster på olika nivåer.

EU Trust Mark visar att den elektroniska förtroendetjänsten har godkännande på EU-nivå

Bedömningar

Coronablinkern bedömdes på rekordtid

Fenomen inom den nationella och internationella säkerhetspolitiken syntes precis som året innan i våra bedömda objekt. Även coronavirussituationen gav sin krydda till vår bedömningsverksamhet. Skyldigheterna och skyddsprinciperna i fråga om internationell säkerhetsklassificerad information skiljde sig inte väsentligt från situationen under normala förhållanden. Å andra sidan kunde vi stöda hanteringen av coronasituationen bland annat genom att bedöma applikationen Coronablinkern som utvecklats av THL för att bryta smittkedjor och informationssäkerheten i bakgrundssystemet. Vi bedömde även flera inhemska krypteringsprodukter för skyddandet av säkerhetsklassificerad information.

Rådgivning om säkra videoförhandlingslösningar och stöd för användningen av molntjänster

Efterfrågan på vår rådgivningstjänst fortsatte sin ökade tillväxt. Utöver skydd för de traditionella miljöerna där säkerhetsklassificerad information behandlas och den kritiska infrastrukturen önskade man att vi ger stöd särskilt i valet och ibruktagandet av säkra videomöteslösningar. Även stödbehovet kring molntjänsterna fortsatte öka. Den uppdaterade versionen av Bedömningskriterierna för säkerheten av molntjänster (PiTuKri) som publicerades i mars togs ivrigt i bruk enligt responsen.

Satellitsystemen syns redan i människornas vardag

Globala satellitnavigationstjänster spred sig i ökande takt i människornas vardag. Satellitpositioneringen är en väsentlig del av de vardagliga tjänsterna och inte enbart ett redskap för att orientera sig från en plats till en annan. Spelindustrin, olika serviceapplikationer, optimering av trafikprestationer, motionsprestationer: i alla dessa spelar satellitpositioneringen en viktig roll.

Satellitpositioneringssystemet Galileo som finansieras av Europeiska unionen har kraftigt klivit fram vid sidan av GPS under 2020 i nästan alla enheter som utnyttjar positionering. Sitt tillägg till förbättringen av positioneringsnoggrannheten och -säkerheten gav även kinesiska BeiDou – som officiellt togs i bruk i augusti 2020 – samt ryska GLONASS.

Ju flera satelliter användarenheten kan ta emot desto bättre är lokaliseringsnoggrannheten. Galileo är det mest exakta av alla globala system och dessutom det enda systemet som erbjuder en mottagningsmöjlighet på två frekvenser i mottagare av konsumentnivå.

Galileo och EGNOS på utvecklingsstigar

I februari nådde Galileo-systemet en ny fas: nödmeddelandetjänsten SAR (Search and Rescue) togs i bruk i full skala. Galileos SAR-tjänst är den första i världen som erbjuder den som skickar nödmeddelandet en automatisk kvittering på att meddelandet nått fram. Även utvecklingsarbetet med andra Galileo-tjänster framskred nästan enligt planerna även om coronavirus fördröjde tidtabellerna något.

Cybersäkerhetscentrets satellittjänster

Våra satellittjänster har diskuterat med GNSS-användarna och lyft fram särskilt de fördelar som Galileo- och EGNOS-tjänsterna ger i framtiden. Vi för en ständig dialog med det inhemska näringslivet för att branschens företag ska kunna bereda sig inför kommande marknadsändringar. Europeiska byrån för GNSS (GSA) har tagits med i diskussionerna.

Under 2020 utarbetades ett beredskaps-program för ibruktagandet av Galileos mest säkerhetskritiska andel, dvs. den offentligt reglerade PRS-tjänsten. Slutresultatet blev en PRS-genomförandeplan som godkändes av alla förvaltningsområden och som fungerar som grund både för projektets finansieringslösningar och den operativa planeringen av tjänsten. I november 2020 drog regeringens ekonomipolitiska minister-utskott upp linjer för att PRS-tjänsten tas i bruk i Finland 2024 och om att man ska bygga den nationella infrastruktur som tjänsten förutsätter från 2021. Byggandet inleds med planeringsarbete och en fastställning av den tekniska arkitekturen under 2021.

Din mobiltelefon är inte ensam!

Se alla Galileo-kapabla enheter.

www.useGalileo.eu

© European GNSS Agency

Galileo ser till att samhället kan fungera!

kyberturvallisuuskeskus.fi/sv/var-verksamhet/satellitnavigation

Samarbete och informationsdelning

Situationsmedvetenheten och informationsdelningen mellan grupperna för informations-utbyte är allt bättre

Medlemmarna i våra grupper för informations-utbyte bildar ett nationellt nätverk med nästan 300 aktörer vars kärnuppgift är att dela sektorspecifik information och erfarenheter av cybersäkerhet och -risker.

Förtroendenätverkens verksamhet har fästs och utvidgats varje år, så även 2020. Särskilt verksamheten för gruppen för informationsutbyte inom trafik och logistik hittade sin rytm och nätverket fick nya medlemsorganisationer.

Grupperna för informationsutbyte har under årens lopp fått en utvecklad situationsmedvetenhet om cybersäkerhet och ett informationsutbyte som även gav oss bättre möjligheter att iaktta och observera branschspecifika cybersäkerhetsdrag.

Den information vi får från grupperna är viktig för att utarbeta lägesbilden för cybersäkerheten. Dessutom är grupperna viktiga för att hantera störningar och främja sektorernas cybersäkerhet.

Distansarbetslösningar, molntjänster och informationshanteringslagen på bordet

Även inom grupperna för informationsutbyte var funktionen och säkerheten hos distansarbetslösningarna och lösningarna för att övervaka distansmiljön uppe för diskussioner. Dessutom diskuterade man informationssäkerheten i videomöteslösningarna, en informationssäker användning av molntjänster och om att se till att organisationens verksamhet och informationssystem följer informationshanteringslagen.

I samarbete med grupperna utvecklar vi bland annat övningsverksamheten för hanteringen av störningar. Ifjol genomfördes en pilotövning för gruppen för informationsutbyte för telebranschens aktörer (ISP-ISAC). År 2021 kommer vi att utvidga förtroendenätens övningsverksamhet. Läs mer om övningsverksamheten på sidan 28.

Grupp för informations-utbyte, på engelska Information Sharing and Analysis Center eller ISAC. Grupperna har grundats för olika sektorer och är cybersäkerhetssamarbetsorgan som baserar sig på tillit.

Cybersäkerhetscentrets grupper för informationsutbyte:

- Statsförvaltningen
- Finans
- Vattenförsörjning
- Telebolag (ISP)
- Social- och hälsovården
- Energi
- Kemi och skogsindustrin
- Livsmedel, handel och distribution
- Media
- Logistik och trafik

Framgångar under året

Många inhemska och internationella informationssäkerhetsgemenskaper omvandlade flera traditionella informationssäkerhetskonferenser till virtuellt format. Förmånliga virtuella evenemang gav särskilt de informationssäkerhetsansvariga vid små finländska företag en unik möjlighet att kunna följa resultaten från aktuell och högklassig informationssäkerhetsforskning. Hoppas att seden fortsätter på ett eller annat sätt även kommande år.

Nätverks- och informationssäkerhetsdirektivets inverkningar och samarbete

Nätverks- och informationssäkerhetsdirektivet NIS fyllde fyra år. Med direktivet regleras informationssäkerheten hos nätverken och informationssystemen, riskhanteringen och beredskapen hos serviceproducenterna som upprätthåller samhällets kritiska branscher. Direktivet innehåller även förpliktelser för de centrala serviceproducenterna att rapportera informationssäkerhetsstörningar. Det är frågan om det första direktivet som reglerar de kritiska funktionernas cybersäkerhet och som just nu håller på att förnyas. Hos oss har NIS-direktivets konsekvenser bäst synts inom de kritiska sektorerna där medvetenheten om informationssäkerheten har ökat. Trots detta finns det ännu brister i kompetensen och tillsynen.

Direktivet gav flera sektorer ett krav på att rapportera betydande informationssäkerhetsstörningar. Det mest betydande fallet 2020 var dataintrånget mot Vastaamo inom hälsovårdssektorn. Fallet ledde till ändringar i regleringen av informationssäkerheten och till åtgärder för att förbättra informationssäkerheten och dataskyddet. Kommunikationsministeriet tillsatte i november en tväradministrativ arbetsgrupp med syftet att kartlägga behovet av att ändra lagstiftningen om informationssäkerheten och dataskyddet hos branscher som är centrala för samhällets funktioner.

Nivån på informationssäkerheten höjs inte bara genom lagtexter

Ingen lagstiftning kan ensam öka informationssäkerheten hos nät eller informationssystem. Företagen ska göra processer och åtgärder som förbättrar riskhanteringen och informationssäkerheten till en del av sin dagliga affärsverksamhet. Tillsynsmyndigheterna ska i sin tur se till att företagens verksamhet och kvaliteten på systemen följer lagen. Preciserande anvisningar, rekommendationer och myndighetsföreskrifter hjälper aktörerna i rätt riktning och vi behöver fler sådana även i Finland.

NIS-direktivet är den första författningen på EU-nivå med syftet att höja nivån på informationssäkerheten inom kritiska sektorer överallt i Europa. Det är frågan om ett långsiktigt arbete som i första hand kräver engagemang hos ledningen men även en aktiv dialog mellan den offentliga och den privata sektorn och ett nära samarbete med myndigheterna.

Blanketten för störningsanmälningar om betydande störningar i nätverk och informationssystem för aktörerna inom samhällets kritiska sektorer:

www.kyberturvallisuuskeskus.fi/sv/anmal

Coronakrisen gjorde den internationella cybersäkerheten elektroniskt

Vi var ordförande i Europeiska unionens CSIRT-nätverk under perioden 1 januari 2019–30 juni 2020. Nätverket arbetade effektiverat och följde upp coronasituationens cybersäkerhetskonsekvenser den 18 mars–6 maj.

De mest betydande iakttagelserna gällde informationssäkerheten i distansarbetsarrangemang, tillräckligheten i kapaciteten för distansförbindelser och användningen av coronatemat i kampanjer för nätfiske och skadliga program. Sjukhus och forskningsinstitut var tydligt föremål för en särskild uppmärksamhet. Efter den effektiverade verksamhetstiden har pandemins internationella läge inom cybersäkerhetskonsekvenserna följts upp genom normalt samarbete.

Coronan har synts i allt samarbete inom våra internationella samarbetsnätverk. Verksamheten har allmänt taget blivit spänstigare och tätare.

I flera internationella gemenskaper har man inte velat pruta på minimiskyddet för säkerhetsklassificerad information även om verksamhetsmetoden delvis saktat upp samarbetet. Undantagstiden har dock även påskyndat processerna för att planera, genomföra och godkänna informationshanteringsmiljöer för säkerhetsklassificerad information.

Övningar ger mer verksamhetssäkerhet

Övningsverksamheten är en av bastjänsterna vårt center tillhandahåller. Vi stöder cyberövningarna för de försörjningsberedskapskritiska organisationerna, deltar i nationella cyberövningar och gemensamma övningar och utvecklar verktyg som stöder övningarna.

Beredskapslagen som riksdagen tog i bruk och uppmaningarna till distansarbete ändrade på cyberövningsverksamheten. Tidigare ordnades majoriteten av cyberövningarna för hanteringen av kontinuiteten som evenemang med närarbete. På grund av coronan måste de som ordnar övningarna och producerar tjänster på kort tid utveckla nya modeller för övningarna som beaktar bland annat distansarbetet och organisationernas osäkra framtidsvyer.

Även inom den närmaste framtiden besvarar vi de försörjningsberedskapskritiska organisationernas behov av övningar, men vi satsar även på att göra våra tjänster skalbara så att så många som möjligt som är intresserade av cyberövningar ska ha nytta av dem. Utifrån den respons vi fick gjorde vi en förutredning om behoven i våra tjänster. Resultatet vet vi våren 2021.

Martti Setälä, Insta Digital Oy:

”Kasta dig modigt in i distansövningarnas värld, det ger belöning.

Antti Nyqvist, Huoltovarmuusorganisaation Digipooli:

”Det är enklare att få fler spelare till en distansövning.

Anu Laitila, Nixu Oyj:

”Involvera alla så jämlikt som möjligt under övningen och testa tekniken innan övningen.

Cybersäkerhetsmärket

Cybersäkerhetsmärket avsett för konsumenternas smarta enheter lanserades i november 2019 med hjälp av tre pilotprodukter. Märket är det första i sitt slag i hela världen som beviljas av en myndighet och väckte redan från början internationellt intresse.

Vi beviljade sex nya märken. Bland dem ingick även två applikationer. En är Coronablinkern som laddats ner 2,5 miljoner gånger och som även ökade kännedomen om Cybersäkerhetsmärket. Internationell synlighet fick vi genom Cybersäkerhetsmärket som beviljades Signifys Philips Hue-smartbelysningssystemet.

Cybersäkerhets märkets utveckling

Våra undersökningar visar att trovärdigheten i Cybersäkerhetsmärket baserar sig på att det beviljas av en pålitlig myndighet. Så kommer det att vara även i framtiden och Traficom äger märket. Då efterfrågan ökar är det viktigt att säkerställa tillgången, därför håller man på att lägga ut de tekniska granskningarna till kommersiella aktörer. De första av dem inleddes i slutet av 2020. Både inhemska och internationella informationssäkerhetsföretag har varit intresserade av att utföra granskningarna.

Då Cybersäkerhetsmärket publicerades baserade de sig märkets krav på ETSIs tekniska specifikation. Utifrån det publicerades världens första officiella IoT-standard i juni 2020. Även Cybersäkerhetsmärkets krav uppdaterades till att motsvara den pinfärska standarden. Cybersäkerhetsmärken som beviljats innan standarden publicerades uppdateras i samband med den årliga granskningen.

Den avgiftsfria Traficom Anycast-tjänsten förbättrar funktionssäkerheten hos .fi-domännamn

År 2020 tog vi i bruk namntjänsten Traficom Anycast för att förbättra funktionssäkerheten hos .fi-domännamn. Vi erbjuder den som sekundär namntjänst för registrarerna av .fi-domännamn – avgiftsfritt – nu och i framtiden. Under vårt Traficom Anycast-webbinarium i oktober berättade vi om tjänsten och dess fördelar för domännamnsregistrarerna.

Traficom Anycast-tjänsten baserar sig på anycast-nätet som administreras av Canadian Internet Authority (CIRA) och som anses vara en av världens mest högklassiga tjänster.

Tjänsten ger extra säkerhet och erbjuder en sammansättning av enheter, programvaror och routrar som gör att namntjänsterna bland annat tål splittrade överbelastningsangrepp bättre än tidigare.

Anycast-tekniken används omfattande i internets rotnamnstjänster samt i .fi-rotnamnstjänsten, men i namnservrarna som fastställts för .fi-domännamnen utnyttjas det extra skydd som anycast-tekniken erbjuder inte i regel.

Skaffa ett .fi-domännamn av en domännamnsregistrar.

Ett fel på namntjänsten lamslår inte bara de digitala tjänsterna utan i värsta fall även all godstrafik och serviceproduktion. Därför lönar det sig att fästa uppmärksamhet vid namntjänstens funktionssäkerhet och informationssäkerhet.

Mer information om ibruktagandet av tjänsten Traficom Anycast får du av din domännamnsregistrar eller av oss på adressen **fi-domain-tech@traficom.fi.**

Namntjänsten eller domain name system, DNS, är ett system på internet som omvandlar domännamnen till IP-adresesr. Tack vare namntjänsten kan vi istället för numeriska adresser använda namn som är lättare att komma ihåg.

Knutpunkterna i anycast-nätet ligger på kartan i Nordamerika, Europa och Asien.

Säkrare 5G med hjälp av lärdomar

År 2019 deltog vi i arrangerandet av världens första hackerevenemang 5G Cyber Security Hackathon som fokuserade på 5G:s informationssäkerhet. I februari 2020 under 5G Leading Edge Forum delade de som ställt upp hackathons utmaningar sina erfarenheter från hackerevenamanget. Det stod klart att vi utan hackathon hade gått miste om information som gör att det går att förbättra säkerheten i 5G-produkterna ytterligare.

I slutet av 2020 tog vi lärdomarna från hackathon och började utarbeta en referensarkitektur för 5G Standalone-näten. Vårt syfte är att beskriva de bästa metoderna för arkitekturen och administrationsprocesserna för säker drift av 5G-nätet. Med referensarkitekturen vill vi besvara de allmänna tekniska hoten som kommer att riktas mot 5G-näten.

Resultaten från referensarkitekturarbetet kommer att testas under 5G Cyber Security Hackathin 2021 där hackers får testa de utarbetade metoderna i en verklig nätverksmiljö. Vi kommer att publicera referensarkitekturen som ett dokument som fritt kan användas av alla operatörer och tillverkare.

KYBER 2020 och den förnyade HAVARO-tjänsten

År 2020 slutfördes Försörjningsberedskapscentralens KYBER 2020-program. Projekten kring programmet, bland annat övningarna, Cybermätaren och KYBER-hälsan, slutfördes. Vi förde även den förnyade HAVARO-tjänsten vidare.

I tjänstens nya modell ordnar kommersiella servicecentrum (SOC) HAVARO-tjänsten för sina kunder i samarbete med oss.

Vi pilottestade den nya servicemodellen under hela året tillsammans med flera servicecentrum och deras kunder. Den kommersiella ibruktagningen av HAVARO-tjänsten sker under 2021.

Under 2021 inleder vi Cyberklimatprojektet med syftet att utveckla vår förmåga att utnyttja data och information för att skapa oss en nationell lägesbild över cybersäkerheten, för att skapa nya tjänster och verksamhetsmodeller och för att besvara cybersäkerhetshot och -avvikelser.

HAVARO

Cybermätaren – Ett nytt verktyg för ledningen för att hantera cyberrisker

Cybermätaren som vi lanserade i oktober har som syfte att förbättra organisationernas och slutligen hela samhällets förmåga att avvärja cyberrisker.

Med hjälp av Cybermätaren får organisationen en vy där de viktiga olika delområdena i cybersäkerheten visas med mål och mogenhetsnivåer. Cybermätaren visar på vilken nivå organisationen klarar av att identifiera, skydda sig mot, iaktta, reagera på och återhämta sig från cyberrisker. Mätaren ger även information om eventuella utvecklingsobjekt, jämförelseuppgifter och ett gemensamt språk för diskussionerna kring cybersäkerheten och hur den kan utvecklas.

I oktober publicerade Försörjningsberedskapscentralen även resultaten från kartläggningen av cybersäkerheten inom olika branscher. Den finskspråkiga utvecklingsversionen av Cybermätaren användes som grund. Den centrala observationen var: Om ledningen engagerar sig och styr cyberstrategin som en del av företagets helhetsstrategi och riskhantering är företaget bättre utrustat för cyberangrepp och kan tackla dem.

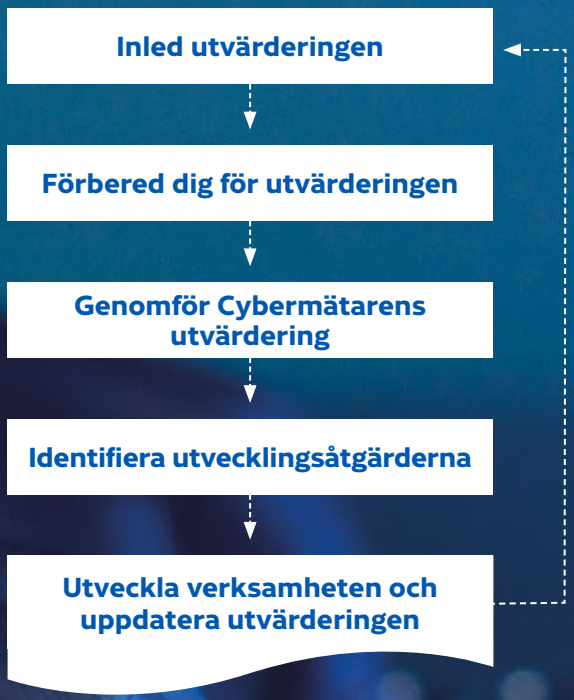
Vid behov kan företagsledningen med hjälp av Cybermätaren få värdefull information om hur den egna beredskapen för cyberrisker förhåller sig till branschgenomsnittet eller andra partner som gjort mätningen. Med hjälp av Cybermätaren kan man även synliggöra mogenheten i den egna leveranskedjan.

Mätaren har många möjligheter: Från konfidentiell informationsdelning till nationell cybersäkerhet

Organisationerna kan välja att dela sina utvärderingsresultat som skapats med hjälp av Cybermätaren konfidentiellt med vårt center. Utifrån dessa resultat kan vi skapa anonymiserade referens- och rekommendationsnivåer som vi kan erbjuda organisationerna som stöd för användningen av Cybermätaren och för utvecklingen av cybersäkerheten. Den här lägesbilden kan vi även utnyttja för att planera och styra nationella åtgärder. Dessutom kan vi utnyttja resultaten konfidentiellt för våra lagstadgade uppgifter och därmed förbättra lägesbilden. Du får mer information om Cybermätaren på vår webbplats.

www.cybermataren.fi

CYBERMÄTARENS UTVÄRDERINGSPROCESS:



”Om ledningen engagerar sig och styr cyberstrategin som en del av företagets helhetsstrategi och risk-hantering är företaget bättre utrustat för cyberangrepp och kan tackla dem.

Nyckeltal för vår verksamhet

Siffrorna tyder på att vårt undantagsår var hektiskt. Nedkörningarna av skadliga webbplatser och antalet fall vi behandlade fördubblades jämfört med föregående år. Gruppen som följer oss på de sociala medierna ökade och våra lägesbildsprodukter var till belåtenhet.

1
Varningar

24/7/365
Oavbruten jour

115 000
Autoreporter

13 353
Twitter-följare

24
Fall som behandlats av sårbarhets-koordineringen

8 500
Nedkörningar av skadliga webbplatser

10 892
Behandlade fall

6 066
Facebook-följare

Antalet störningar

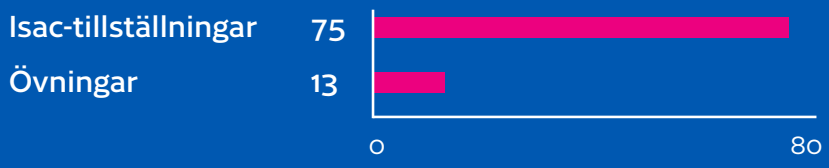
4
Kritiska störningar

12
Allvarliga störningar

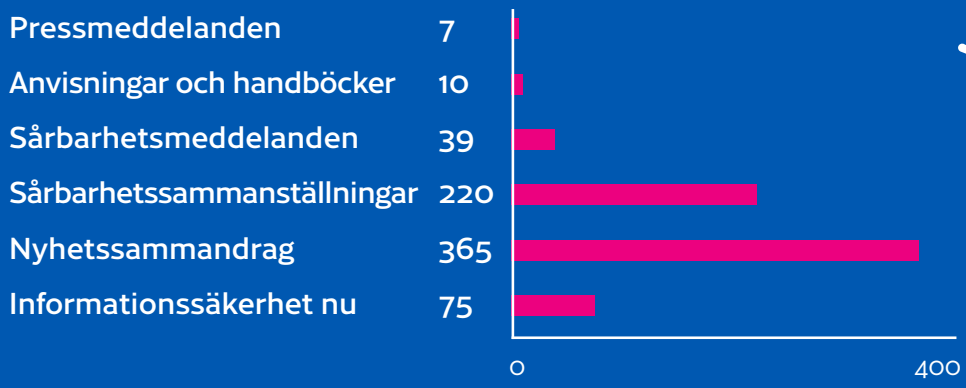
51
Betydande störningar

67
Alla störningar totalt

Tillställningar och övningar



Kommunikation och meddelanden



Under året genomförde vi kundnöjdhetsenkäter om våra lägesbildsprodukter och om våra grupper för informationsutbyte. Skalan för bedömningen i våra enkäter var från dåligt (1) till utmärkt (5).

4,4
Nytta

Våra lägesbildsprodukter är till belåtenhet

4,2
Genomsnitt

Enkät till branschernas grupper för informationsutbyte

4,5
Vitsord

Cybervädret 2020 och blicken mot 2021

10 informationssäkerhetsutsikter för 2021

1. Det inträffar något otrevligt även 2021

Många organisationers riskhantering håller inte takten med digitaliseringen. Man tar i bruk lösningar helt i blindo utan att ha utvärderat, eller förstått, riskerna med dem. Slutresultatet kan vara uselt både för medborgaren, organisationen och hela samhället. Cyberåret 2020 var trist men vi förutspår mörka moln även för det kommande året.

2. Mer reglering, mer stabilitet

Lite solsken skulle göra gott i det regniga cybervädret. Man strävar allt mer efter att kontrollera cybersäkerhetsriskerna med nationell och multinationell reglering. Kraven ökar särskilt inom sektorer som är viktiga för samhällets funktion. Man vill även stoppa handeln med data, bland annat folks hälsoinformation, med hjälp av reglering. Detta kan även leda till att stora teknoföretagsjättar splittras upp i mindre bitar.

3. Det blir svårare att skilja det äkta från det förfalskade

Deepfake och andra lösningar som baserar sig på artificiell intelligens erbjuder möjligheter att fördunkla vår informationsomgivning ytterligare. Populisterna och bråkstakarna inom den internationella politiken använder möjligheten till sin fördel utan nåd.

4. Det tar ännu länge att få upp kompetensen på tillräcklig nivå

Efterfrågan på de proffs som det digitala samhället behöver ökar. Samma gäller experter inom informationssäkerhet och dataskydd. Behovet har identifierats och riktningen i utvecklingen av utbildningen är rätt, men ändringen sker långsamt.

5. Brottslingarna grävde virtuell valuta med cyberangrepp

I Finland sker allt fler nätangrepp och tiotusentals av dem är småpengar. Ett särskilt betydande hot är angrepp med utpressningsprogram där vem som helst kan bli offer, alla från små verkstäder till internationella high tech-jättar.

6. Distansarbetet har kommit för att stanna – samma gäller för riskerna

År 2020 gick vi supersnabbt över till att jobba på distans. En del av aktörerna byggde i brådskan upp sina distansarbetsarrangemang på brokiga lösningar. Det kommer att ta länge att få den här massan i skick.

7. Tävlingen om en kvanthållbar kryptering ökar i takt

Kvantdatorerna är 2021 ännu lite mer utvecklade. Informationssäkerhetsindustrin förbereder sig idogt på kvantdatorernas era. Kvanthållbara krypteringslösningar ökar i jämn takt.

8. Den teknologiska stormakts-konkurrensen trappas upp

Inverkan av den teknologiska stormakts-konkurrensen sträcker sig även till telefon- och applikationsbutikernas hyllor. Kinesisktillverkade Huawei vs. amerikanska iPhone – hurdana tekniker och applikationer kan man använda i de här enheterna i framtiden?

9. Cyberpåverkan mellan staterna fortsätter öka

Cyberangrepp, spridning av disinformation och hybridpåverkan ökar. Påverkan och angreppen i cybermiljön är ofta billigare och mer obemärkt på nätet än i den fysiska världen.

10. Cybersäkerheten äntligen på ledningens agenda

Fallet Vastaamo lyfte upp cybersäkerheten och dataskyddet på ledningens agenda. Utvecklingen förutsätter dock långsiktighet eftersom cybersäkerhetshoten ständigt förändras. Vår Cybermätare är ett utmärkt verktyg som snabbt ger ledningen en översikt över nivån på organisationens cyberförmåga.

Cybervädret 2020

Januari

Föreskrift 66 om störningar i televerksamheten trädde i kraft.

Spionaget riktas inte bara mot staterna utan även mot företagen.

Februari

Office 365: Ständigt fiske efter användarnamn, ökat antal dataintrång.

Bedrägerisamtal från falsk teknisk support: Finländarna har fått hundratusentals samtal. Antalet fall ökar explosionsartat.

Certifikatstörningar: Microsoft glömde förnya sina certifikat vilket orsakade störningar i Teams-tjänsten.

EKANS – det första utpressningsprogrammet riktat mot automationssystem upptäcktes i världen.

Mars

Coronan: Försäljning av obefintliga coronaskydd och -testpaket. Människornas nöd utnyttjas i spridningen av skadliga program, i bedrägerier och spionage.

Bedrägerisamtal från falsk teknisk support: Samtalen upphörde den 24 mars.

Dataläckage från olika stamkundssystem. Även uppgifter som tillhör finländare hamnar i fel händer.

April

Coronan: Vaccinforskning som eventuellt spionagemål.

Telias störning i internetförbindelsen den 25 april.

Maj

Posti-bedrägerierna: Tusentals textmeddelanden har skickats i Postis namn som leder till prenumerationsfällor, fiske eller skadliga program.

Utpressningsangrepp: Utpressarna auktionerade ut information de stulit.

Gruppen Sandworm försökte tränga sig in i sårbara Exim-e-postservrar redan 2019/08.

Ett angrepp med utpressningsprogram mot ett inhemskt system för kritisk infrastruktur.

Juni

Bedrägerisamtal från falsk teknisk support: Samtalen började igen.

Angrepp med den skadliga programvaran EKANS riktades mot Honda och ENEL Group.

Flera kritiska sårbarheter som bland annat inverkade på VPN-tjänsternas informationssäkerhet.

Toppsiffror: 12 betydande kommunikationsnätsstörningar, tre av dem orsakades av stormen Päivö.

= Internationell nyhet

Bedrägerisamtal från falsk teknisk support: Samtalen fortsätter. Hundratusentals samtal till Finland.

Certifikatstörningar: DigiCert anullerade flera certifikat den 11 juli. Det inverkade på funktionen hos flera finländska tjänster.

Iakttagelser av finländska servrar där intrång gjorts eller som har sårbara VPN-program.

Rikligt med kritiska sårbarhets-publikationer. Säkerhetshålen i nätenheterna utnyttjades i hög grad.

EU satte för första gången sanktioner mot nationella cyberangripare.

En ny våg av utpressnings-program. Flera iakttagelser av utpressningsanfall mot hälsovårdssektorn ute i världen.

Zerologon-sårbarheten utnyttjas aktivt.

Stormen Aila: 9 betydande funktionsstörningar som snabbt ficks under kontroll.

Iakttagelser av att hotet om överbelastningsangrepp ökar.

Office 365: Fler dataintrång, fiskemeddelanden skickas från de drabbade e-postlådorna.

Antalet Emotet-fall har minskat och varningen avlägsnades därför.

Dataläckage i Estland, flera ministerier utsatta.

Informationssäkerhetsbolaget FireEye och Europeiska läkemedelsverket utsatta för spionage.

Juli | Augusti | September | Oktober | November | December

VARNING 1/2020: Den skadliga programvaran Emotet sprids aktivt i Finland.

Norges parlament utsätts för dataintrång. Norge beskyllde Ryssland för cyberangreppet.

Den första officiella standarden för IoT-konsumentenheternas informationssäkerhet publicerades.

Den globala Century-Link störningen den 30 augusti. Hela internettrafikens volym minskade med 2 procent.

Office 365: Fiske efter användarnamn med trovärdiga Zoom-möteskallelser.

Psykoterapicentret Vastaamo: Företaget och kunderna utpressades genom hot om att publicera patient- och personuppgifter.

Anmälningar om omfattande överbelastningsangrepp som även syns i tjänsternas funktion.

En bakdörr hittades i hanteringsverktyget SolarWinds – möjligheter till dataintrång och spionage.

Säkerhetsister – informationssäkerhetens medborgarkampanj inleddes.

Riksdagens dataintrång i nyheterna.

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

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

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

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

Anmäl en informationssäkerhetskränkning till oss
www.kyberturvallisuuskeskus.fi/sv/anmal

Transport- och kommunikationsverket Traficom
Cybersäkerhetscentret

PB 320, 00059 TRAFICOM
tfn 029 534 5000

cybersakerhetscentret.fi

ISBN 978-952-311-764-8
ISSN 2669-8757

TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret