# Informationssäkerhet

## 2018

TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

# INNEHÅLL

# Cybersäkerhet angår alla

2018 var ett år av förändringar. Under sommaren flyttade vi till nya lokaler i Gumtäkt och i slutet av året blev vi en del av det nya Transport- och kommunikationsverket TRAFICOM. Efter mycket positiva, men även arbetsamma, erfarenheter kan vi år 2019 koncentrera oss fullt ut på att utveckla vår verksamhet.

Säkerhetskulturen i Finland grundar sig på ett stadigt samarbete mellan den privata och den offentliga sektorn. Ett liknande samarbete har jag inte stött på någon annanstans i världen.

Det finns utan tvekan många orsaker till samarbetstraditionen. För det första känner de som arbetar i informationssäkerhetbranschen i Finland varandra väl – namn kopplas snabbt ihop med bekanta ansikten. Det är lättare att lita på någon man känner. Att samarbetspartnerna känner ett stort förtroende för varandra är den andra faktorn som stöder samarbetet. För det tredje upplever samarbetspartnerna uppriktigt att de drar nytta av samarbetet.

Samarbetet är en enorm resurs för oss. Våra samarbetspartner förser oss behändigt och smidigt med mycket konfidentiella uppgifter utan lagstadgat tvång. En sak vi prioriterar är ansvarsfull hantering av konfidentiella uppgifter. Enligt den respons vi fått från våra intressenter är det smidiga och tillförlitliga samarbetet vår viktigaste styrka, utan att glömma vår yrkeskompetens. Dessa ska vi värna även i framtiden.

Likväl kan samarbetet förbättras. Vi måste se till att vi inte stänger in oss i en bubbla av enbart informationssäkerhetsfolk, utan att även medborgare drar nytta av resultaten av vårt samarbete.

De många cybersäkerhetshoten kan sakta men säkert skada vårt förtroende för digitala miljöer om vi inte längre känner oss säkra och upplever att vi inte längre har kontroll. Problemen kring Office 365 som spred sig i sakta mak och fiskade efter användaruppgifter blev det största informationssäkerhetshotet 2018. Vi får inte glömma bort eller underskatta vikten av den mänskliga aspekten av informationssäkerhet. Cybersäkerhet kan inte bli vardagsmat för medborgarna om vi inte informerar om den på ett mänskligt och förståeligt sätt. Jag hoppas att så många som möjligt känner till Turvalisti-Teijo samt lösenordsgeneratorn Pidempi parempi (Ju längre desto bättre). Genom 2018 års kampanjer riktade till medborgarna ville vi få ut budskapet om informationssäkerhet till alla.

Vårt mål är att utveckla det inhemska cybersamarbetet så att det fungerar mer sammanflätat i framtiden. Tanken är att bygga upp en helhet kring vår tjänst HAVARO så att hotinformation kan spridas och bearbetas effektivt. Med hjälp av ett tätare samarbete är det möjligt att bättre skydda de kritiska tjänster som tillhandahålls medborgarna, eftersom skyddet mot informationssäkerhetshot och återställandet efter dem skulle ske snabbare än i dagsläget. Jag tror att med hjälp av ett ”cyberekosystem” kan både den privata och den offentliga sektorn producera elektroniska tjänster där användarna – oavsett om det är barn, unga, vuxna eller äldre – kan känna sig trygga.

*Alla behövs för detta gemensamma projekt. Välkommen med!*

Helsingfors den 31 januari 2019,
**Jarkko Saarimäki**
Direktör
Cybersäkerhetscentret
Transport- och kommunikationsverket Traficom

# CENTRALA INFORMATIONS-SÄKERHETSHOT OCH HUR MAN SKYDDAR SIG MOT DEM

## TOP5 hotbilder och lösningar för privatpersoner och organisationer

# PRIVATPERSONER

## HOT

**Kriminella försöker stjäla dina användaruppgifter**
Med de stulna användaruppgifterna kan de försöka få åtkomst till exempelvis offrets e-postkonto. E-posten är nyckeln till många ställen eftersom den används för att återställa lösenord för många nättjänster.

**Nätbedrägerier hör till vardagen på webben**
I synnerhet falska nätbutiker och abonnemangsfällor lurar pengar av konsumenter. Även bedrägerier i form av utpressning med känsligt material via e-post och falsk teknisk support har dykt upp.

**Bristfälligt skyddade enheter**
Många smarttelefoner, datorer och IoT-apparater för hemmet som erbjuds konsumenter har obefintlig informationssäkerhet: de använder standardlösenord och tillgången till produktstöd och uppdateringar är dålig. De hör inte hemma på internet – de är ett hinder i kommunikationstjänsternas funktion.

**Falska appar i officiella appbutiker**
Appar som installerats på telefonen kan vidareförmedla mer information än vad du har tillåtit och rentav spionera på dig och stjäla dina uppgifter.

**Värdefulla uppgifter läcker ut från nättjänster**
Uppgifter om användare och betalningar läcker hela tiden ut från genuina nätbutiker och sociala medier, och kriminella kan utnyttja dessa bland annat i sina bedrägeriförsök.

## LÖSNINGAR

**Ge inte appar onödiga rättigheter**
Det går oftast att redigera en apps rättigheter även efter att den installerats. En ficklampa fungerar utan åtkomst till din kontaktlista eller dina bilder.

**Kontrollera om meddelandet och dess bilagor är äkta**
Bluffmeddelanden kan skickas som e-post, textmeddelande, samtal eller privatmeddelande i sociala medier. Om du är misstänksam, verifiera att meddelandets innehåll är riktigt till exempel per telefon.

**Lösenordsgeneratorer och tvåfaktorsautentisering**
Det är svårt att komma ihåg tillräckligt långa och säkra lösenord. Använd tvåfaktorsautentisering (2FA/MFA) i synnerhet för e-post, sociala medier och de vanligaste molntjänsterna då det är möjligt.

**Skydda dig med hjälp av säkerhetsprogram**
Brandvägg och antivirusprogram kommer ofta i samma paket. Använd dem. Följ även varningar och anvisningar de ger.

**Kontrollera fakturan för ditt kreditkort regelbundet**
Var särskilt uppmärksam efter att du har handlat på nätet eftersom dataintrång hos genuina nätbutiker har blivit allt vanligare. Vid behov kan du döda ditt kort. Tänk på att en it-brottsling inte åker fast om du inte gör en polisanmälan.

# ORGANISATIONER

## HOT

**Kriminella försöker sko sig på dina uppgifter**
Bedragare och nätfiskare vill komma åt organisationens informationssystem och utnyttja uppgifterna de kommer över. Vissa bedrägerier är mycket trovärdiga och väl riktade, och kan orsaka kännbara ekonomiska förluster.

**Utkontrakterade tjänster är ytterligare en väg in för angriparen**
En angripare kan komma åt företaget via dess samarbetspartners och underleverantörers system, i synnerhet om företaget lägger ut sina centrala tjänster på entreprenad och även tillhandahåller dem för sina samarbetspartner. Angrepp eller störningar i systemen kan få stor spridning och till oanade platser, om företaget inte kan kontrollera sina egna tekniska miljöer.

**Bristande insyn**
Det är inte nödvändigtvis så att man känner den egna miljön tillräckligt väl. Det är mycket svårt att lägga märke till angrepp och lokalisera dem om man inte samlar in loggdata i tillräcklig utsträckning. Till exempel utnyttjar attacker sårbarheter i programvara nästan direkt efter att information om sårbarheten har gått ut till allmänheten.

**Värdefulla uppgifter aktiverar spioner**
I Finland är politiska beslut, spetsteknologi och innovationer av intresse. Även politiska val kan väcka intresse utomlands. Till exempel under perioden som EU:s ordförandeland är Finland ett potentiellt föremål för nätspionage och påverkan. Utöver medierna aktiveras även hacktivister och politiska grupperingar.

**Överbelastningsangrepp hör till vardagen**
Varje organisation ska vara beredd på överbelastningsangrepp.

## LÖSNINGAR

**Inkludera ansvar för informationssäkerhet i avtal**
Genom utkontraktering kan du få yrkesmässig informationssäkerhetskompetens utanför din kärnverksamhet. Ansvar kan inte utkontrakteras utan att de har beaktats i avtalet.

**Grundläggande hygien för enheter och programvara**
Underhåll och uppdatera alla enheter som är anslutna till nätet. Skapa en rutin för regelbunden uppdatering och säkerhetskopiering.

**Utbilda, öva och testa**
Genom att öva testar man verksamheten och kan hitta utvecklingsområden. Att samla in lärdom om egna incidenter är en väsentlig del av beredskapen.

**Förankra informationssäkerhet som arbetsgemenskapens arbetssätt**
Informationssäkerhet ska beaktas i hela verksamheten. Den ska vara en del av den övergripande riskhanteringen och beredskapen.

**Känn ditt system och dina tjänster**
Då är underhåll och beredskap effektivt; loggning är en väsentlig del av detta. Överväg automatisering om det gör arbetet mer effektivt och förbättrar processernas verksamhet.

# DE VIKTIGASTE CYBERSÄKERHETSFENOMENEN

## Bedragare vilar inte

## Från e-postkonton till bluffakturor

Bedrägeriåret 2018 har färgats av utpressning, nätfiske via Office 365 och VD-bedrägerier. Abonnemangsfällor och nätfiske efter bankuppgifter är kända fenomen sedan tidigare och visar inga tecken på att avta. Det dyker bara upp allt fler bedrägerier.

Något man säkert kommer att minnas från 2018 är nätfisket efter användaruppgifter till e-posttjänsten i Microsoft Office 365. Fenomenet är inte nytt; man har alltid försökt komma åt olika organisationers konton. Hittills har nätfiske förutsatt ett tidskrävande bakgrundsarbete där gärningsmannen har satt sig in i varje organisations fjärranvändargränssnitt separat. Nu har den populära molnbaserade Office-tjänsten förenhetligat olika organisationers e-posttjänster. Samtidigt har även nätfiske blivit enklare: samma bluffmeddelande går hem hos flera organisationer som använder samma tjänst.

Vi gick ut med en kritisk varning om nätfiske i juni 2018 när hundra e-postkonton hos tiotals organisationer hamnade i fel händer. Från konton som hamnat i händerna på kriminella skickades tusentals nya bluffmeddelanden vidare och årets värsta våg av nätfiske drog likt en lavin från organisation till organisation.

Kapade e-postkonton användes även för att begå andra brott. Kriminella kunde följa trafiken på kontona och kom över organisationernas interna uppgifter. Med hjälp av dem förberedde man faktureringsbedrägerier, förfalskade fakturor och bland annat organisationen själv och dess kunder lurades på pengar.

## Bedrägerier och bluffar

Nätbedragarnas uppfinningsrikedom tar aldrig slut. All slags information kan missbrukas, till exempel för utpressning. Olika lösenordsläckor har kommit till nätanvändarnas kännedom när urgamla listor med lösenord till tjänster som man glömt för många år sedan kommer upp till ytan. Om man har tillräckligt många föråldrade lösenord kan man enkelt skrämma folk att tro att alla deras övriga uppgifter också har stulits.

I utpressningsmeddelanden som sprids globalt via e-post och som har visat sig vara en bluff kombineras lösenord från gamla läckor med en anklagelse om att mottagaren har tittat på porr. Även om bedragaren inte alls har något känsligt material om sitt offer, ökar den slumpmässiga gamla lösenordsläckan bluffmeddelandets trovärdighet: Betala eller så berättar jag allt om dig!

*”Kriminella kunde följa trafiken på kontona och kom över organisationernas interna uppgifter.*

## Bluffmeddelanden till mobila enheter

Vi surfar allt oftare på nätet från mobila enheter. Även bedragarna har flyttat dit och kontaktar sina offer även via textmeddelande. Bluffmeddelanden skickas så väl till e-postkonton som till smarttelefoner. En webblänk som finns i ett textmeddelande kan leda till en abonnemangsfälla eller nätfiske precis som webblänkar i e-postmeddelanden.

Konsumenten lockas in i en abonnemangsfälla med falsk markandsföring och löften om lotterivinster. Kända varumärken, tv-apparater och mobiler för ett par euro är vanligt förekommande i dessa. Under förevändning av ett lotteri eller en leveransavgift luras konsumenten att lämna ut sitt kreditkortsnummer. Något pris ser man inte skymten av, men konsumenten märker att hen har bundit sig till en viss tjänst och att en månadsavgift debiteras hens kreditkort.

## Finns det något som hjälper mot bedrägerier?

Vi informerar allmänheten om rådande faror på internet genom att gå ut med informationssäkerhetsvarningar. Våra varningar har blivit väl uppmärksammade och de har effektivt tagit sig över mediernas nyhetströskel. Vissa potentiella offer har sannolikt kunnat undgå fara, men tyvärr har alltför många gått i fällan. I synnerhet organisationer måste själva ta ansvar för att upplysa sin personal och hålla dem underrättade om farorna med till exempel bedrägerier. I egenskap av myndighet tillhandahåller vi all möjlig hjälp.

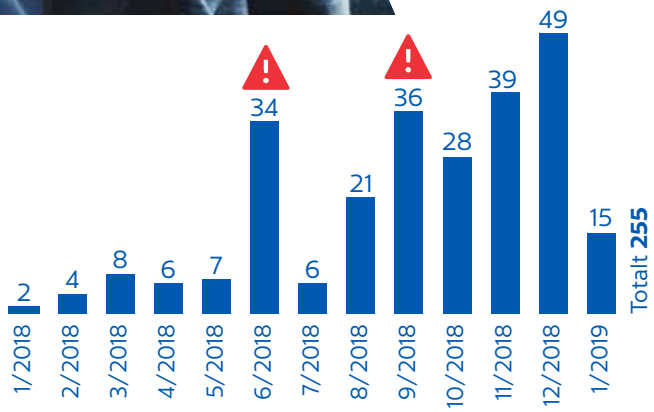
# Brott planeras allt mer ingående

Det gångna året har på många sätt varit en ögonöppnare även för polisen. Bedrägeribrotten på nätet i Finland har traditionellt skett på inhemska handelsplatser, i form av e-postbedrägerier och så kallade nigeriabrev. Under året har man dock stött på ett nytt omfattande fenomen: nätfiske via Microsoft Office 365.

Tillvägagångssätten varierar något, men en allmän iakttagelse är att gärningsmannen sätter sig in i den brottsliga gärningen mer noggrant och i större detalj än tidigare. I praktiken är det fråga om ett datainträng, varefter det egentliga bedrägerimönstret planeras utifrån information man kommit över från e-post eller en annan tjänst.

Nätfisket via molntjänsterna är i själva verket en förlängning på de VD-bedrägerier som man redan sett under en längre tid och som globalt sett har medfört förluster på hundratals miljoner euro. Genom internationellt samarbete har man också lyckats få fast vissa gärningsmän. En bedragare som kunde gripas som ett resultat av samarbetet mellan polisen i Israel, Frankrike och Belgien samt FBI hann lura till sig 1,2 miljoner euro. I Finland pågår tiotals brottsutredningar. Förlusterna uppgår till hundratusentals euro.

**Tomi Liesimaa**
Centralkriminalpolisen




*Antalet tickets i anslutning till Office 365 18 januari – 19 januari. Tydliga toppar i juni, september samt i november och december.*

## 2017

**8/2017** Vi fick en anmälan om nätfiske via Office 365-konton och informerade om det.

## 2018

**2/2018** I februari–mars 2018 börjar Office 365-observationer igen dra till sig uppmärksamhet.

**11.6** Vi gick ut med en kritisk varning.

**8.8** Varningen sänktes från kritiskt till allvarlig.

**21.9** Varningen höjdes igen från allvarlig till kritisk.

**26.9** Tvåfaktorsautentiseringen kringgicks.

**4.10** Bluffmeddelanden kamouflerades som säkra e-postmeddelanden.

**26.10** Varningen sänktes igen från kritisk till allvarlig.

**27.11** Fler drabbade: Hundra personers användaruppgifter stals via en nätfiskelänk i en PDF-bilaga.

**11.12** Inloggning med regionala begränsningar kringgicks med hjälp av VPN-anslutningar.

**20.12** Bluffmeddelanden kamouflerades som meddelanden om röstmeddelanden.

**28.12** Bluffmeddelanden spreds via SharePoint-sidor.

## 2019

**1/2019** I januari 2019 var situationen fortsättningsvis allvarlig.

# Olika skeden av nätfiske via Office 365

I juni 2017 observerades många e-postmeddelanden som syftade till nätfiske i Finland. Kampanjen var främst riktad mot företagsledningen och personer som arbetar med it-underhåll. Efter att man lyckats komma över användaruppgifter till den molnbaserade e-posttjänsten Office 365 Exchange Online som organisationerna använder, har man till exempel skapat olovliga e-postregler som skickar meddelanden vidare och som det är svårt att lägga märke till med vanliga underhållsverktyg.

I augusti 2017 uppmanade vi folk att se till att hålla användaruppgifterna säkra och i vår artikel i Informationssäkerhet nu! gav vi anvisningar för hur man inför tvåfaktorsautentisering eftersom man ofta fiskar efter just lösenord. Redan i september varnade vi för riktat nätfiske. I november meddelade vi om problemet igen eftersom fenomenet inte verkade avta.

I februari 2018 försökte vi – än en gång – göra organisationerna uppmärksamma på situationens allvar. Vi publicerade en artikel i Informationssäkerhet nu! med exempelbilder på nätfiskesidor med Office 365- och OneDrive-tema. Vi varnade även för PDF-dokument i omlopp som innehöll en länk till en nätfiskesida.

Trots vår aktiva kommunikation fördubblades antalet fall som kom till vår kännedom. I juni beslöt vi att gå ut med en kritisk varning, eftersom organisationer som använder Office 365 måste agera för att få bukt med problemet! Varningen fick stor uppmärksamhet och synlighet i massmedierna, men fenomenet försvann ändå inte, utan fortsatte än värre.

I september 2018 märkte vi att det inte räcker med tvåfaktorsautentisering om systemet tillåter att man kringgår det på en äldre terminal. I oktober började även bluffmeddelanden kamouflerade som säkra e-postmeddelanden sprida sig. Office 365-bedragarna verkade bara bli allt fler, och nya offer vilseleddes att lämna ut sina användaruppgifter till de kriminellas nätfiskesidor.

Till och med slutet av året hade antalet anmälda fall av nätfiske inte minskat i någon större omfattning och därför gäller varningen fortfarande.

# Sårbarheter och skadliga program

*”Observationerna av skadeprogram på hemmaroutrar och IoT-apparater utgör nästan 60 % av Cybersäkerhetscentrets alla observationer av skadeprogram.*

## Sårbarheterna hölls i schack och epidemier kunde undvikas

Ett viktigt sårbarhetsfenomen år 2018 hörde ihop med sårbarheter som hittats i processorer av olika tillverkare.

Härvan fick sin början i januari när sårbarheterna Spectre och Meltdown visade att en angripare kan komma åt uppgifter i ett annat program eller operativsystem som körs med samma processor. På grund av Spectre och Meltdown undersöktes processorers sårbarhet mer runtom i världen och ett stort antal nya fall hittades också. Sårbarheterna i processorer har i synnerhet påverkat molnbaserade miljöer och andra fleranvändarmiljöer, men vissa av dem gäller även vanliga hemanvändare.

Under det gångna året hittades även många kritiska sårbarheter i operativsystemens nätverkslösningar. Sårbarheterna gällde Windows, Unix, MacOS och FreeRTOS – i praktiken alla operativsystem. Genom att utnyttja de olika sårbarhetstyperna var det möjligt att åstadkomma till exempel ett överbelastningsangrepp. Med hjälp av det allvarligaste säkerhetshålet kunde angriparen skriva egen programkod i målsystemet. Eftersom det inte genast fanns ett effektivt sätt att utnyttja sårbarheterna kunde dock epidemier som sprider sig i form av internetmaskar undvikas.

## Skadliga program bryter virtuell valuta, klickar på reklam och gör intrång i nätbanker

Åren 2017 och 2016 var det mycket ståhej kring not-Petya, WannaCry och Mirai, år 2018 var det mindre. Utpressningsprogram som krypterar datorns hårddisk och kräver en lösensumma för att häva krypteringen dök upp för flera år sedan, men trots våra prognoser har dessa minskat i antal.

Istället för utpressningsprogram genererar it-brottslingar inkomster genom att bryta virtuell valuta med sitt offers datorresurser. Skadliga program som bryter virtuell valuta har vi också observerat i Finland. Det mest uppmärksammade fallet drabbade Lahtis stads it-system i början av året: det självspridande skadliga programmet WannaMine som bryter virtuell valuta. En brytare kan även smygas in i programkoden på en webbplats varvid angriparen nästan obemärkt lyckas bryta valuta i besökarens webbläsare. Offrets dator behöver inte ens nödvändigtvis smittas med ett skadligt program.

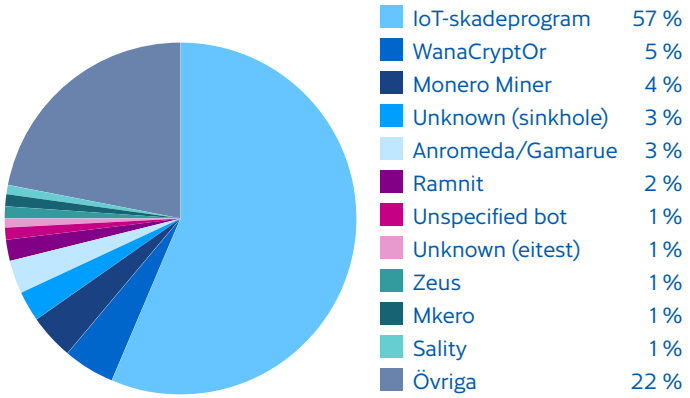
Skadeprogrammen Kovter och Emotet som spridits globalt har vi även sett i Finland. Kovter är ett skadeprogram som ”klickar” på reklam på nätet som gör att en webbplats på konstgjord väg kan öka sina reklamintäkter. Emotet däremot är ett mångsidigt skadeprogram som till exempel stjäl användaruppgifter eller laddar ner andra skadliga program.

*”Om det inte är möjligt att regelbundet uppdatera en enhet ska den kopplas bort från internet.*

## Spridning via e-postbilagor, routrar och datorer som inte uppdaterats

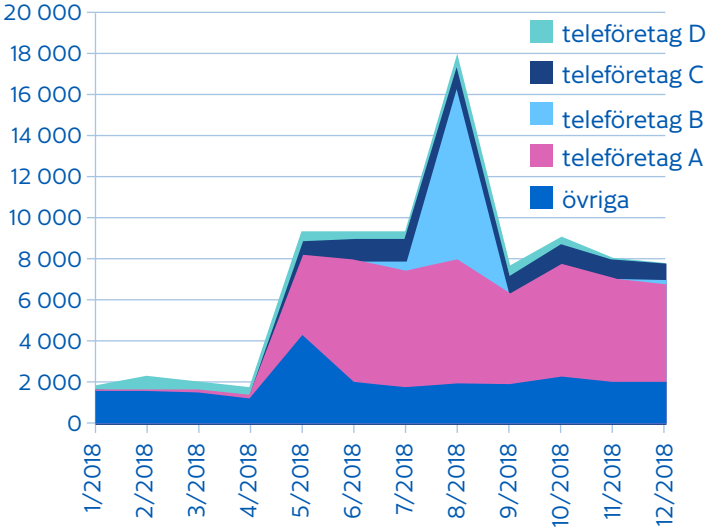
År 2018 var bilagor till e-postmeddelanden det absolut vanligaste sättet att sprida skadliga program. Ofta består bilagan av ett dokument som innehåller makron som sprider skadeprogrammet till datorn.

Vi observerade att antalet hemmaroutrar infekterade av skadliga program ökade betydligt under sommaren 2018. Observationerna gällde i synnerhet vissa modeller av hemmaroutrar från några teleföretag. Just nu utgör skadliga program på olika hemmaroutrar och andra IoT-apparater en stor del, nästan 60 procent, av alla observationer av skadliga program som anmäls till oss.




*IoT-skadeprogram utgör nästan 60 procent av alla våra observationer av skadliga program 2018.*

> *”Observationerna av skadeprogram på hemmaroutrar och IoT-apparater utgör nästan 60 % av Cybersäkerhetscentrets alla observationer av skadeprogram.*




*Allt fler observationer av IoT-skadeprogram gjordes 2018. Observationerna är koncentrerade till några teleföretag. En topp i augusti 2018.*

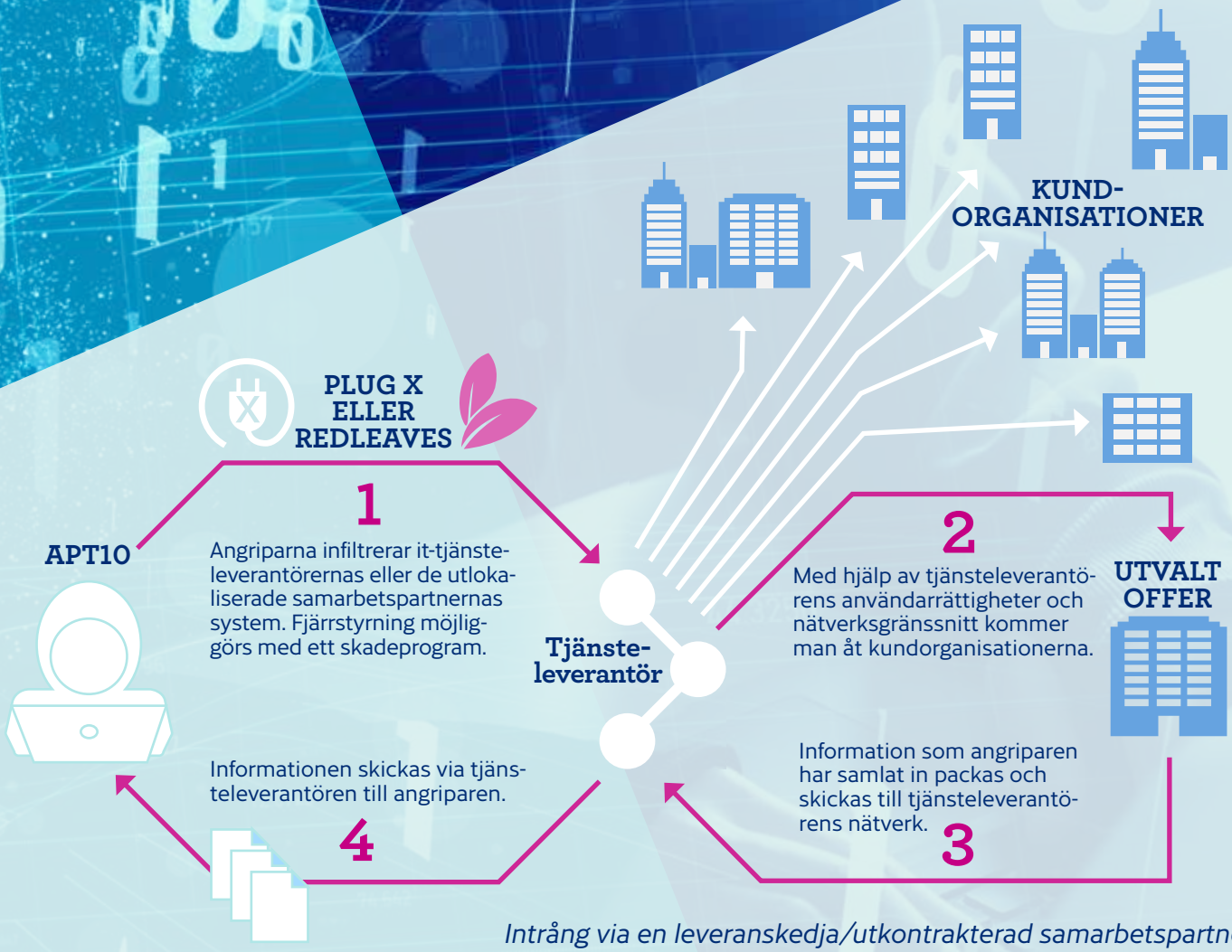
Vi gör fortfarande observationer även om mycket gamla skadeprogram. Till exempel ser vi fortfarande skadeprogrammet Zeus som hittades år 2007. Fenomenet är typiskt och beror troligen på att vissa datorer inte uppdateras eller startas om. Efter installationen har underhållet av dessa enheter glömts bort, och därför utgör de en lämplig jordmån för infektioner av olika slags skadliga program.

Oavsett om det handlar om ett storföretags webbserver eller en webbkamera för hemmabruk ska alla apparater som är anslutna till internet underhållas och uppdateras. Om det till exempel inte är möjligt att regelbundet uppdatera en enhet ska den kopplas bort från internet.

Kriminella söker hela tiden efter sårbara enheter på nätet. En enhet som är ansluten till internet och har en sårbarhet som det är allmänt känt hur man utnyttjar blir snabbt hackad. En hackad enhet kan till exempel delta i överbelastningsangrepp, bryta virtuell valuta eller skicka skräppost.

# Spionage och påverkan

*”Det är inte längre endast vanlig ”kontorsdatateknik” som är utsatt, utan även automationssystem som driver livsviktiga funktioner i samhället.*




*Intrång via en leveranskedja/utkontrakterad samarbetspartner*

*Källa: BAE Systems Threat Research Blog
https://baesystemsai.blogspot.com/2017/04/apt10-operation-cloud-hopper_3.html
https://2.bp.blogspot.com/-sBNjr4znWk/WN573Vvsfml/AAAAAAAAAno/OKLwDezpCF-gLwQt8k-EfvG7Ptn6nETefACLcB/s640/infographic.png

## På spionagefronten intet nytt

Redan år 2017 övergick man från spionage till påverkan och missbruket av leveranskedjor var uppenbart. Samma fenomen höll sig kvar även 2018.

Utöver nätspionage, dvs. olovligt inhämtande av information via datanät, ville angriparna dessutom lamslå eller störa de utsatta it-systemens verksamhet. Målen varierade från industriautomation till OS-tävlingar. I vissa fall hade inget egentligt sabotage ens utförts, utan syftet var att bland annat skapa fotfäste för eventuella kommande operationer.

År 2018 diskuterades flera fall i offentligheten där dataintrång hade använts som stöd för militära operationer. Både Rysslands och USA:s försvarsorganisationer pekades ut. Cyberintrång verkar ha blivit en permanent del av militära angrepp.

## Angrepp mot automationssystem och offentliga anklagelser mot angripare

Intrång i informationssystem på olika sätt och i olika syften är centrala redskap i verktygsbacken för dagens hybridpåverkan. Det är inte längre endast vanlig ”kontorsdatateknik” som är utsatt, utan även automationssystem som driver livsviktiga funktioner i samhället. I förberedelserna för störningar och undantagssituationer bör man även beakta metoder för att avvärja en målmedveten statlig aktör.

Ett klart undantag till detta är att politiska beslutsfattare är mer villiga att offentligt anklaga andra stater och rentav enskilda tjänstemän för konstaterade dataintrång. I synnerhet USA och Storbritannien har ofta anklagat såväl Rysslands som Nordkoreas underrättelsetjänster för olika dataintrång. Men det har varit turbulent även i Europa när Belgien anklagade Storbritannien för intrång i en belgisk teleoperatörs informationssystem.

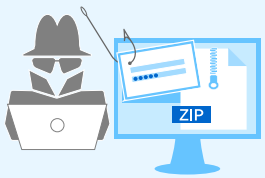
Utifrån enbart tekniska bevis är det nästan omöjligt att vattentätt bevisa exakt vem som har suttit framför angriparens tangentbord och varför angreppet har gjorts. I synnerhet anklagelser som görs i offentligheten grundar sig ofta på politiska beslut eller riktlinjer.

# Dagens företagspionage är svårare att upptäcka än tidigare

År 2018 kom dataintrång via leveranskedjor att bli allt mer framträdande i spionage riktat mot företag. Via uppdateringsservrar och it-underhållstjänster är det möjlig att göra intrång mot flera mål samtidigt. Det är betydligt svårare att lägga märke till angrepp via leveranskedjor än till exempel riktad skadlig e-post.

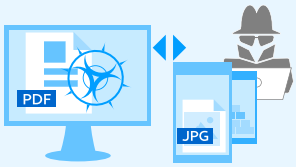
För att till exempel EU-kommissionen ska kunna ingripa i statliga aktörers företagsspionage måste företagen göra en bedömning av de ekonomiska förlusterna till följd av cyberangrepp. Bedömningen bör utöver direkta kostnader även omfatta indirekta kostnader. Direkta kostnader är till exempel kostnader i anslutning till utredning av dataintrång och nya it-system. Indirekta kostnader är däremot förluster till följd av stöld av immateriell egendom och förlorade affärsmöjligheter.

**1 RIKTAT NÄTFISKE-MEDDELANDE**



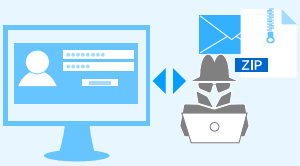

Ett e-postmeddelande innehåller en länk eller en bifogad fil, vanligen ett Word-dokument.

**2 DET FÖRSTA SKEDET UTFÖRS**



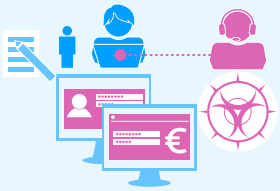

Ett makro i Word-dokumentet startar PowerShell.

**3 POWERSHELL**



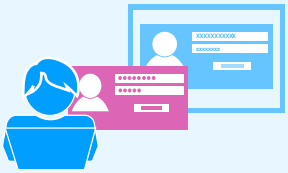

Anslutning till angriparens ledningsserver.

**4 SPIONAGE DEL 1**



Datainsamling via datanät och it-system.

**5 UTÖKADE BEFOGENHETER**

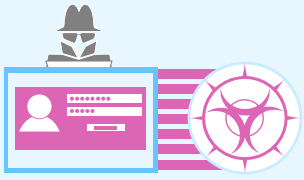


Angriparen skaffar mer omfattande befogenheter.

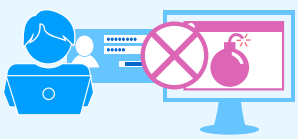
**6 SPIONAGE DEL 2**

Kritiska system identifieras.

**7 INSTALLATION AV SKADEPROGRAM**



**8 AKTIVERING AV SKADEPROGRAM**



Hårddiskar skrivs över, system lamslås och affärsverksamheten störs.

*Hur ett intrång framskrider. I det sista skedet har dataintrånget lyckats.*

*Källa: IBM X-Force IRIS Team
https://securityintelligence.com/the-full-shamoon-how-the-devastating-malware-was-inserted-into-networks/

# Överbelastningsangrepp

*”Den genomsnittliga storleken på överbelastningsangrepp fortsätter att öka i jämn takt. I slutet av 2018 var det redan fullt normalt att angrepp även mot enskilda konsumenter var > 10 Gbps. Angrepp som använde Memcached kom för att stanna, men de har till all lycka inte genererat några stora problem efter att den första vågen drog in. Angreppen ökar fortfarande och ser inte ut att avta, så därför är det bra att vara beredd på de problem som överbelastningsangrepp medför.*

**Osmo Soinio**
Telia

## Vem som helst kan köpa ett överbelastningsangrepp mot ett önskat mål

Så kallade stresser-tjänster som erbjuder överbelastningsangrepp tillhandahåller även kortvariga, kostnadsfria demonstrationsangrepp. Statistiken visar att majoriteten, cirka 75 procent, av alla överbelastningsangrepp i Finland pågår i mindre än 15 minuter. Eftersom dessa angrepp är så kortvariga men ändå så många, handlar det troligtvis om kostnadsfria demonstrationsangrepp av stresser-tjänster.

Till följd av en internationell polisoperation i april stängdes tjänsten webstresser.org som utförde överbelastningsangrepp på beställning. Det var frågan om världens största dos-tjänst och när den stängdes minskade antalet angrepp internationellt. Likväl finns det fortfarande ett stort antal tjänster på nätet där man kan beställa överbelastningsangrepp mot en önskad webbadress.

Vanligen pågår överbelastningsangrepp så länge som de har en inverkan på föremålets verksamhet. I allmänhet slutar angriparen när överbelastningsangreppet avvärjs och tjänstens verksamhet återställs. Ofta byter angriparen däremot bara mål och angreppet fortsätter mot någon annan tjänst i samma målorganisation.

Överbelastningsangreppen som förekommer i Finland har vanligen en volym på omkring 1–10 Gbit/s. Med dessa volymer kan man i allmänhet påverka tjänstens verksamhet om det inte finns särskild beredskap för överbelastningsangrepp. Varje vecka inträffar flera angrepp på över 10 Gbit/s i Finland. Det största angreppet mot Finland som vi fick kännedom om år 2018 hade en styrka på cirka 90 Gbit/s och pågick i flera timmar.

*”cirka 75 procent av alla överbelastningsangrepp i Finland pågår i mindre än 15 minuter.*

## Angreppen mot identifieringstjänsten suomi.fi syntes tydligt

Under sommaren och hösten gjordes flera överbelastningsangrepp mot identifieringstjänsten suomi.fi som påverkade många statliga tjänsters verksamhet negativt. Identifieringstjänsten är en central komponent i många andra tjänster och är därför ett attraktivt mål även för angripare.

Angreppen mot suomi.fi var kanske det mest synliga exemplet på överbelastningsangrepp men de var inte de enda. År 2018 gjordes sammanlagt flera tusen överbelastningsangrepp i Finland. Man kan säga att överbelastningsangrepp har blivit vardag och sker hela tiden. Alla angrepp får dock inte lika synliga konsekvenser för tjänsternas funktion, vilket vi kan tacka organisationernas goda beredskap för.

*”År 2018 gjordes sammanlagt flera tusen överbelastningsangrepp i Finland.*

## Angreppsmetoderna är så gott som oförändrade

I genomförandet av överbelastningsangrepp används olika metoder och de vanligaste är reflektionsattacker samt nättrafik som skickas från hackade terminaler. Ofta kombineras också dessa metoder. I en reflektionsattack används servrar på nätet, till exempel namnservrar eller CLDAP-katalogtjänster, för att förstärka belastningstrafiken. År 2018 utfördes ännu fler reflektionsattacker också med hjälp av felkonfigurerade memcached-servrar.

## Det går inte att skydda sig mot angrepp utan framförhållning och planering

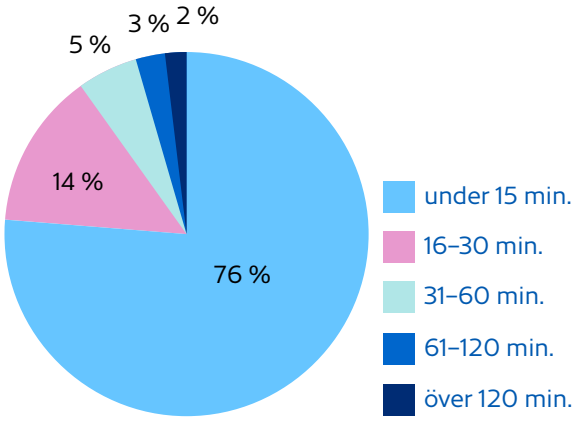
Organisationer ska beakta överbelastningsangrepp i sina riskbedömningar. Om till exempel åtkomsten till företagets tjänster på internet är viktig, måste man planera för hur man skyddar sig vid ett överbelastningsangrepp och förbereda sig i god tid.

Olika typer av angrepp kräver olika slags skydd. För att skydda sig mot angrepp på applikationsnivå ska nättjänsten utformas så att den är svår att belasta genom enskilda förfrågningar såsom komplicerade databassökningar. För att vara förberedd på angrepp som skapar flera TCP-anslutningar ska webbarkitekturen, belastningsfördelningen och innehållsförmedlingen utformas så att inte tjänsten stockas av att det skapas många sessioner samtidigt. Med hjälp av tjänster som köps från teleföretag, till exempel brandvägg eller paketfilter, kan man bekämpa volymbaserade angrepp.

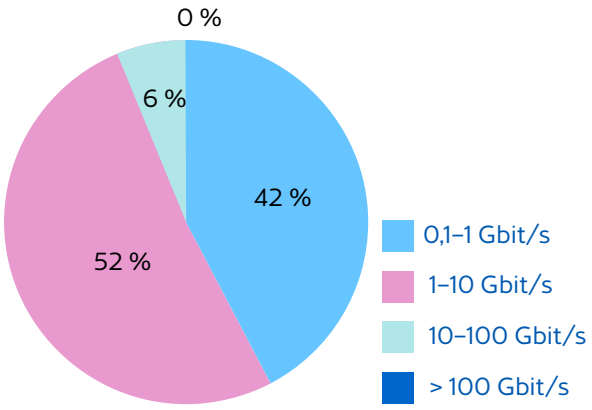
Det finns därför ingen patentlösning för hur man skyddar en nättjänst. Utformningen av nättjänsten ska som helhet sikta på att kunna uthärda olika slags angrepp och återhämta sig snabbt efteråt.

*”Av informationssäkerhetshoten är ett överbelastningsangrepp det mest synliga vad gäller förhållandet mellan pris och kvalitet, men i allmänhet inte det allvarligaste. Det kan jämföras med en organiserad demonstration framför en kontorsbyggnad: det drar till sig uppmärksamhet och hindrar kunder från att komma in. I värsta fall kan ett angrepp försätta människoliv i fara om det blockerar kritiska tjänster.*

**Jarna Hartikainen**
Chef
Traficom/Cybersäkerhetscentret




*Tidsmässig varaktighet för överbelastningsangrepp riktade mot Finland år 2018 (källa: Telia).*




*Volymer för överbelastningsangrepp riktade mot Finland år 2018 (källa: Telia).*

# Driftsäkerheten hos inhemska kommunikationsnät

*”De senaste åren har samarbetet mellan Cybersäkerhetscentret och teleoperatörerna förbättrats avsevärt och blivit mer öppet. Operatörerna träffar varandra regelbundet bland annat i Transport- och kommunikationsverkets olika arbetsgrupper där man behandlar hur störningssituationer ska hanteras och förebyggas. Fall och situationer där man med tanke på samhällets funktion har nytta av att samarbeta kommer fram på ett naturligt sätt i grupperna. Perspektivet är bredare än en enskild operatör.*

*En snabb återhämtning efter störningar, att samhällets kritiska tjänster fungerar och att det finns beredskap ligger i allas intresse. Fungerande tjänster gagnar oss alla och därför lönar det sig – trots konkurrensen – också för operatörerna att samarbeta till exempel i omfattande tekniska störnings- och undantagssituationer.*

*Idag deltar även elbolagen och räddningsverken i samarbetet. Nu kan vi bättre sörja för att medborgarna har så välfungerande kommunikationstjänster som möjligt till sitt förfogande.*

**Tomas Lång**
DNA Abp

## Situationen blir bara bättre

Under de senaste åren har det skett allt färre stora störningar i de inhemska kommunikationsnäten, och denna trend fortsatte även 2018. Väderförhållandena orsakade de längsta störningarna i näten, men genom samarbete mellan teleföretag och elbolag hölls konsekvenserna på en måttlig nivå jämfört med tidigare år och reparationerna framskred effektivt.

Teleföretagen underrättade oss om sammanlagt nästan 70 betydande funktionsstörningar. Av dessa var cirka 14 mer allvarliga och omfattande. Antalet störningar har minskat med omkring en tredjedel jämfört med året innan. Dock förekom det fler störningar i allvarlighetsklass A än året innan. Däremot inträffade inte ens hälften så många störningar i allvarlighetsklass B som året innan.

Cirka hälften av felen i klass A gällde markbunden tv och oftast orsakades störningarna av fel i utrustningen. Även ändringsarbeten i teleföretagens nät, utrustning och programvaror orsakade avbrott i kommunikationsnätets tjänster.

## Samtal och internet fungerade, driftssäkerheten hos kritiska system måste förbättras

I början av 2018 drabbades ett område i Kajanaland av omfattande strömavbrott som varade mellan ett par dagar till över en vecka i vissa fall. Räddningsverket i Kajanaland tog själv det allmänna ledningsansvaret för situationen, vilket säger något om störningarnas omfattning och allvar. Strömavbrotten påverkade även kommunikationstjänsternas funktion, men stora störningar kunde undvikas. Till exempel fungerade nödsamtal och de som deltog i räddningsarbetet kunde använda mobiltelefonnätet för att dela information.

De inhemska kommunikationsnätens funktion har förbättrats de senaste åren. En anledning är teleföretagens förnyade nätkonstruktioner där en omfattande störning inte längre kan uppstå när en enskild länk bryts. De positiva konsekvenserna av nätförändringarna kan ses i statistiken för år 2018 som en minskning av antalet betydande störningar. År 2018 förekom störningar på enskilda nät som orsakade avbrott i de viktigaste tjänsterna för samhället. Till exempel utgjorde störningar i telekommunikationsnäten för ett sjukhus och ett trafikstyrningssystem ett hinder för att använda tjänster i anslutning till dessa. Beredskap för avbrott och störningar i kritiska system ska skapas i god tid, redan när dessa upphandlas och avtalas.

## Teleföretagen var mer aktiva att anmäla informationssäkerhetsskränkningar

Antalet informationssäkerhetskränkningar eller hot om kränkningar varierar från år till år, men i genomsnitt får vi in 1–2 anmälningar om betydande fall varje månad. Så var även fallet 2018. Majoriteten av fallen gäller dataintrång i it-system eller olovlig användning av it-system, sårbarheter i teleföretags system eller stora överbelastningsangrepp som gjorts via teleföretagens nät.

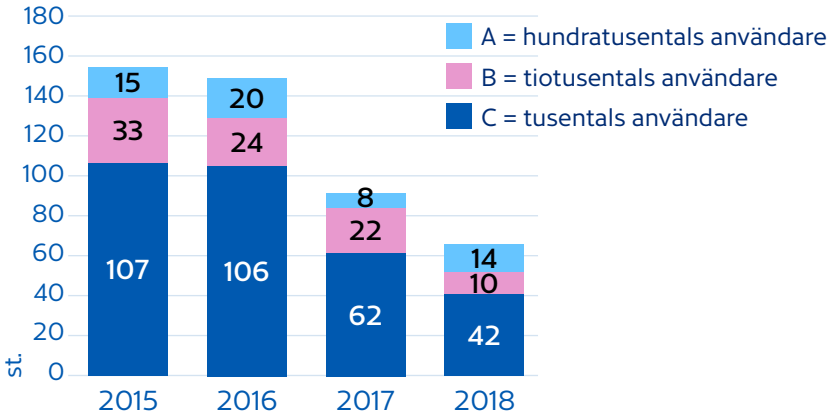
De senaste åren har antalet anmälningar om informationssäkerhetskränkningar gällande personuppgifter som vi tagit emot ökat kraftigt. Det är osannolikt att själva antalet kränkningar av personuppgifter håller på att öka. Det är snarare så att teleföretagen nu bättre känner till i vilka situationer informationssäkerheten gällande personuppgifter kan kränkas och att alla sådana situationer ska anmälas.

Den vanligaste typen av informationssäkerhetskränkning gällande personuppgifter är fel i hanteringen av kunduppgifter. I dessa fall behandlar teleföretaget sina kunders personuppgifter felaktigt så att en kunds personuppgifter avslöjas för en annan. Till exempel, i samband med en beställning av en ny anslutning får en kund av misstag en kopia av anslutningsavtalet för den kund som betjänades före honom. Det är också möjligt att när en kund vill flytta förfallodagen för sin anslutningsfaktura och tar kontakt med teleföretaget per telefon eller chat, sparas fel telefonnummer i kundens kontaktuppgifter varvid meddelandet som bekräftar att förfallodagen flyttats skickas till en annan kund.

Sedan år 2002 har vi samlat in information om betydande informationssäkerhetskränkningar eller hot om kränkningar mot teleföretagens kommunikationsnät och -tjänster. En kränkning eller ett hot bedöms vara betydande utifrån i synnerhet skydd av beställares och användares rättigheter, tjänstens användbarhet och geografiska konsekvenser.

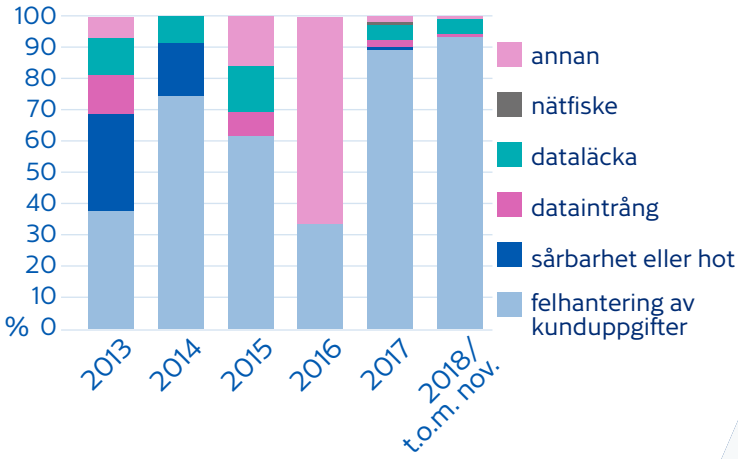
Sedan år 2013 har teleföretagen även anmält informationssäkerhetskränkningar gällande personuppgifter till det nuvarande Transport- och kommunikationsverket. Anmälningarna gäller huvudsakligen fall där personuppgifter förstörs, försvinner, ändras eller lämnas ut av misstag eller olovligen.

## Antalet betydande driftsstörningar i olika allvarlighetsklasser




*Det totala antalet betydande störningar (A–C) per år har minskat allt sedan år 2015. Under år 2018 inträffade färre mindre fel i klass C, medan det inträffade fler fel i klass A än under år 2017.*

## Typer av kränkningar av personuppgifter




*”De positiva konsekvenserna av nätförändringarna kan ses i statistiken för år 2018 som en minskning av antalet betydande störningar.*

# Sakernas internet

*”Den enskildes problem blir ett gemensamt problem när oskyddade och illa hanterade apparater kapas och används till exempel för överbelastningsangrepp.*

## Dataläckor, olovlig observation och överbelastningsangrepp

Sakernas internet, Internet of Things (IoT), växte under år 2018 till att bli en ännu större del av konsumenternas vardag. Apparater som övervakar sin omgivning och förmedlar information om den underlättar konsumentens liv till exempel genom att styra hemmets belysning och uppvärmning eller genom att rapportera om sömnkvalitet och puls. Med de nya IoT-innovationerna spred sig beklagligt nog även informationssäkerhetsproblem i anslutning till apparaterna.

Bristerna i informationssäkerheten i dessa konsumentprodukter syns bland annat i form av dataläckor och intrång i privatlivet. Fallen visar att endast ett fåtal kan bedöma och hantera informationssäkerheten för de nätanslutna och informationssparande apparater som används i hemmet. Den enskildes problem blir ett gemensamt problem när oskyddade och illa hanterade apparater kapas och används till exempel för överbelastningsangrepp. När kritiska och offentliga tjänster digitaliseras kan angrepp mot IoT-apparater försvaga hela samhällets funktion.

Tills vidare finns det inga allmänt erkända eller förpliktande informationssäkerhetskrav för IoT-apparater och därför är det svårt att förebygga brister i informationssäkerheten. Den snabba teknologiska utvecklingen har gjort det svårare att förstå riskerna med apparater och tjänster på djupet. Lagberedningen en har också gått långsamt, men situationen verkar så småningom förändras till det bättre.

## Brister under kontroll genom reglering, informationssäkerhetsstämpel för säkra apparater

I september 2018 fastställde delstaten Kalifornien vad som troligen är världens första informationssäkerhetslag för sakernas internet. Även internationella standarder för sakernas internet och dess informationssäkerhet är under beredning. Lättare riktlinjer på principnivå har tagits fram under året i bland annat Tyskland och Storbritannien.

I Finland har Transport- och kommunikationsverket Traficom följt utvecklingen av den internationella regleringen. Informationssäkerhetsproblemen med IoT-apparater verkar öka i en snabbare takt än kraven som ställs på apparaterna. Därför har verket börjat utveckla en stämpel för informationssäkerhet som ska hjälpa konsumenten att identifiera informationssäkra apparater och göra säkra val. Eftersom det är dyrt att lägga till egenskaper för informationssäkerhet i efterhand och ofta också svårt, är tanken med stämpeln också att uppmuntra tillverkare att planera apparater som är informationssäkra under hela livscykeln. Detta kallas secure by design. I konsumentprodukter tillämpas denna idé redan till exempel i Ikeas smarta belysning Trådfri.

# Riskbedömningar av informationssäkerhetsfenomen

# Stora informationssäkerhetsrisker för privatpersoner, organisationer och statsförvaltningen

Här bedömer vi de största riskerna i anslutning till stora cybersäkerhetsfenomenen 2018. Vi har lyft fram exempelfall på hur riskerna har kunnat se ut för privatpersoner, företag, kommunala organisationer eller statsförvaltningen. Pilens riktning berättar hur situationen har utvecklats jämfört med 2017. Vår uppfattning är att den allmänna risknivån för cybersäkerheten i Finland 2018 hölls så gott som oförändrad jämfört med år 2017. I samband med vissa fenomen har riskerna ökat.

▶ Risken den samma
▲ Förhöjd risk

| | PRIVATPERSONER | ORGANISATIONER | STATEN |
|---|---|---|---|
| BEDRÄGERIER OCH NÄTFISKE | ▲ Nätfiske efter bankkoder och kreditkortsuppgifter sker ofta. Bedrägerier och utpressning är mycket vanliga. | ▲ Användarkonton hos molntjänster har råkat ut för en mängd nätfiskekampanjer. | ▶ VD-bedrägerier och faktureringsbedrägerier drabbar även statsförvaltningen. |
| ÖVERBELASTNINGSANGREPP | ▶ Hackade hemmaroutrar och andra IoT-apparater används bl.a. för att utföra överbelastningsangrepp. | ▶ Överbelastningsangrepp hör till vardagen. Avvärjningen av angrepp måste planeras så att organisationens nättjänster hålls fungerande. | ▶ Överbelastningsangrepp hör till vardagen. Både egna nättjänster och nättjänster som köpts av en tjänsteleverantör måste skyddas. |
| SKADLIGA PROGRAM OCH SÅRBARHETER | ▲ Skadliga program infekterar snabbt oskyddade IoT-apparater som anslutits till internet. | ▲ Oskyddade servrar som anslutits till internet hittas och hackas. Skadliga program sprids i e-postbilagor. | ▶ Skadliga program sprids i e-postbilagor. |
| SPIONAGE | ▶ Personer behandlar politiskt känsliga ämnen och är aktiva på sociala medier kan råka ut för nätspionage. | ▲ Spionage mot företag inom den kritiska infrastrukturen verkar ha ökat. | ▶ Statsförvaltningen är fortsättningsvis ett väsentligt föremål för nätspionage. |
| SAKERNAS INTERNET, IOT | ▶ Privat information avslöjas via oskyddade apparater som är anslutna till nätet. Apparater kan även utnyttjas i botnät. | ▲ Genom att utnyttja säkerhetsbrister hos IoT-apparater kan man komma över nätverksresurser. Uppgifter om enheter och användare kan hamna i händerna på angripare även från offentliga källor. | ▲ Oskyddade IoT-apparater innebär även en ryktesrisk. Via till exempel smartklockor är det möjligt att följa militärers rörelser och position. |
| KOMMUNIKATIONSNÄT | ▶ Användningen av digitala tjänster ökar, trots det är man inte helt beroende av att de fungerar. God förmåga att klara av korta störningar. | ▲ Störningarna minskar men beroendet av digitala tjänster ökar. Eftersom beredskapen för störningar är bristfällig sprider sig konsekvenserna också till konsumenterna. | ▲ Beroendet av digitala tjänster ökar. Varierande beredskap för störningar. |

# CYBERSÄKERHETSCENTRET STÅR TILL TJÄNST

## Rådgivning och tillsyn för informationssäkra miljöer

*”Behovet av informations-säkerhetsrådgivning har ökat märkbart.*

## Lärdomar av utvärdering av informationssäkerhet 2018

Det fanns enorma skillnader i de objekt som utvärderades under året, också behovet av rådgivning om informationssäkerhet var tydligt. Liksom tidigare år såg vi i vår utvärdering av it-system att skyddsnivån varierar avsevärt. Även utvärderingsobjektens skala var omfattande.

Det minsta objektet vi utvärderade var en fristående dator som var fysiskt separerad från övriga datorer och nätverk. Då koncentrerade vi oss på att utvärdera den administrativa och fysiska säkerheten samt metoder för skydd mot i synnerhet elektromagnetiska läckor och skyddsmetoder i produktionsprocessen. När det istället var fråga om en it-systemhelhet som används i flera länder och av olika organisationer bedömde vi särskilt säkerhetshantering samt skydd i anslutning till säkerheten i leveranskedjor.

I vårt arbete blev det klart att behovet av informationssäkerhetsrådgivning tydligt har ökat. Man behövde råd om såväl hur man effektiv skyddar it-systemen som hela samhällets cybersäkerhetsberedskap. Man behövde i synnerhet stöd i anslutning till planering av it-system och identifiering av risker för organisationer.

## Mot en bättre företagssäkerhet

Vårt mål är att tillsammans med bedömningsorgan för informationssäkerhet förbättra företagssäkerheten. Samarbetet har redan tagit sina första steg och god praxis skapas efterhand.

Samarbetet utvecklas planenligt bland annat med hjälp av en årsklocka. Syftet med den är att göra verksamheten mellan organisationerna regelbunden, öka kontakterna, ge utbildning, förenhetliga handlingsätten och – kanske det viktigaste – skapa diskussionskontakter.

**1 Allokera resurser och se till att det finns kompetens**

Organisationer allokerar inte tillräckligt med resurser för informationssäkerhet. Utan sakkunskap är det nästa omöjligt att sörja för verksamhetens säkerhet och upprätthålla den. För att undvika att göra för mycket eller för lite bör planeringen av informationssäkerheten särskilt för systemen som stöder verksamheten skötas av sakkunniga.

**2 Identifiera objekt och kritisk information som ska skyddas**

Om information som ska skyddas inte identifieras eller definieras, ökar både risker och kostnader för att genomföra tjänsterna. I värsta fall får man okontrollerade arkitekturlösningar. Detta är möjligt till exempel om ett objekt som ska skyddas inte har separerats tillräckligt från övriga system.

**3 Tjänster kan inte genomföras på ett informationssäkert sätt om man inte har den kompetens som krävs**

När man utkontrakterar tjänster ska man se till att skyldigheter och ansvar som man kommit överens om med tjänsteleverantören är tillräckliga och har definierats noggrant. Till exempel om tjänsteleverantören inte levererar uppgifter som behövs i en undantagssituation för att åtgärda situationen, kan uppdateringar försummas och hanteringsförbindelser som inte är informationssäkra användas.

**4 Händelser, incidenter och loggar i det egna nätet ska följas upp**

Även om man faktiskt sparar systemloggar, är det inte säkert att loggarna är tillräckligt omfattande. De kanske inte följs upp eller har till exempel så motsägelsefulla tidsstämplar att nödvändig information inte kan utredas.

**5 Verifiera informationssäkerhetsnivån i systemen**

Någon bedömning har kanske inte gjorts över huvud taget eller så ligger ansvaret för den hos ett företag som säljer bedömningstjänster på kommersiella grunder. Då kan man ifrågasätta huruvida bedömningen är oberoende. Bedömningar som utförts av Cybersäkerhetscentret eller ett godkänt bedömningsorgan för informationssäkerhet ger en oberoende bild av systemets säkerhet.

## Galileo fick finländska satellitkunniga i rörelse

Det gångna året var arbetsamt, i synnerhet arbetet med att samordna cybersäkerheten i EU-samarbetsorgan. I egenskap av ordförandeland står vi bland annat värd för det gemensamma mötet för EU-ländernas PRS-myndigheter i september i Helsingfors.

De europeiska Galileo-satelliternas räckvidd är nu global. Detta har även gjort att fler kunniga i Finland vill vara med och bygga upp den nationella delen av PRS-tjänsten. Vi tog upp ämnet i en workshop i november där sammanlagt 80 representanter för myndigheter och företag för kritisk infrastruktur deltog.

År 2018 skapades ett inhemskt PRS-samarbete med bland annat Geodatacentralen och försvarsmakten. Också spektrumförvaltningen vid vårt verk håller på att intensifiera samarbetet.

I Finland torde EU:s eget satellitbaserade positioneringssystem Galileo tas i bruk i början av 2020-talet. Med hjälp av systemet kan man skydda sig bättre än i dagsläget mot bland annat GPS-störningar. I november förekom det störningar i Lappland på grund av Natos storövning.

## Smidig handledning och verkningsfull tillsyn

När den används rätt är reglering ett bra verktyg för att förbättra cybersäkerheten och kännedomen om störningar.

År 2018 har informationssäkerhet och beredskap tagit en allt större plats i lagberedningsarbetet. Ändringen har i synnerhet kunnat ses i lagstiftningen om säkerhet i samband med elektroniska tjänster eller hantering av viktig information i nätverks- och informationssystem. Inriktningen har varit välkommen, men även sysselsatt vårt center med förfrågningar om konsultationer och utlåtanden.

Under årets andra hälft behandlade vi 50 begäranden om utlåtande. Var och en av dessa gällde någon aspekt av cybersäkerhet, informationssäkerhet eller beredskap. Våra experter har varit bekanta gäster såväl i arbetsgrupper som i riksdagens utskott.

*”År 2018 har informationssäkerhet och beredskap tagit en allt större plats i lagberedningsarbetet. Under höstsäsongen behandlade vi 50 begäranden om utlåtande.*

*Bilden föreställer en Galileo-satellit. PRS, dvs. Public Regulated Service, är en tjänst för positions- och tidsinformation för myndighetsanvändning via satellitpositioneringssystemet. I varje EU-land finns en PRS-myndighet som administrerar användare och ansvarar för genomförandet av nyckelfördelningen. I Finland har Transport- och kommunikationsverket Traficom denna uppgift.*

## Ett måste att vara insatt i hur EU:s regleringsprojekt framskrider

Ändringar i lagstiftningen sker inte över en natt. En väsentlig del av arbetet är att följa i synnerhet ändringar i EU-lagstiftningen och att vara beredd på dessa. Under det gångna året har vi aktivt följt bland annat totalreformen av regelverket för elektronisk kommunikation som senast ändrades 2009, beredningen av EU:s förordning om integritet och elektronisk kommunikation (ePrivacy) och EU:s cybersäkerhetsförordning. För att inte tala om ändringarna i regleringen av förtroendenät och stark autentisering som kommunikationsministeriet började bereda i brådskande ordning under hösten.

På våren slutfördes ett viktigt EU-projekt när kraven enligt nät- och informationssäkerhetsdirektivet (det så kallade NIS-direktivet) trädde i kraft. Direktivet ställer minimikrav för uppföljning och rapportering om informationssäkerhet på samhällets kritiska branscher och på grund av det får vi i fortsättningen mer omfattande information från olika branscher om situationen beträffande informationssäkerheten. Denna information kan användas i utvecklingen av cybersäkerheten i framtiden.

Skyldigheterna att rapportera om informationssäkerhet och störningar gäller nu även digitala tjänster, dvs. molntjänster, sökmotorer och internetbaserade marknadsplatser. Informationssäkerhetsskyldigheterna som föreskrivs i NIS ska följas i sektorerna för energi, transport, finans, hälso- och sjukvård och distribution av dricksvatten. Vi bjöd in tillsynsmyndigheterna för dessa branscher till en arbetsgrupp där styrning, kunnande och tillsyn kan samordnas. Tillämpningen av direktivet granskas också tillsammans med tillsynsmyndigheter för övriga medlemsstater.

## Med siktet på säkra elektroniska tjänster

Regleringen har inte varit lika snabb som till exempel utvecklingen av programvara år 2018, och därför försöker vi vara så smidiga som möjligt i våra föreskrifter och övriga styrning. Vi förutser och bedömer vad lagstadgade krav innebär i praktiken för de företag som omfattas av vår tillsyn och för samhället i övrigt. Allt detta tar tid. Ett öppet samarbete har varit värdefullt för oss, men även nödvändigt eftersom vi med hjälp av den information vi fått på detta sätt har kunnat beakta de praktiska kraven i utvecklingen och tolkningen av regleringen.

Vi lyssnar och beaktar, men är även krävande. Alla måste följa de föreskrivna kraven, men vi gör upp föreskrifter och ger råd i tolkningen av regelverken så att aktörer vet vad som krävs av dem och vad de kan förbättra. På detta sätt kan vi hjälpa aktörerna som omfattas av vår tillsyn att utveckla tillförlitliga tjänster.

Vi tar till tillsynsmetoder vid behov. Mot slutet av året drev vi på ännu de sista som tillhandahåller stark autentisering att sluta använda TLS 1.0. Under det gångna året träffade våra experter även många regionnätsaktörer i samband med kontroller av att kommunikationsnätens säkringar följer föreskrifterna.

# Samarbete och informationsdelning

## I grupperna för informationsutbyte lär man sig mest

Samarbete och informationsutbyte med statsförvaltningen och försörjningsberedskapskritiska företag är en central del av Cybersäkerhetscentrets verksamhet. I synnerhet i grupperna för informationsutbyte, (ISAC, Information Sharing and Analysis Centre), vars verksamhet vi samordnar, är samarbetet som mest intensivt.

Viktiga branscher för samhällets funktion har egna ISAC-grupper där man försöker hitta lösningar på informationssäkerhetsproblem i branschen samt delar information om aktuella cyberhot och -fenomen. Samarbetet gagnar de organisationer och myndigheter som deltar i gruppen, men framför allt medborgarna. Vi stöder organisationer som tillhandahåller tjänster som är kritiska för samhället och viktiga för medborgarna att sörja för underhåll och utveckling av informationssäkerheten i sina affärslösningar.

I dagsläget finns det 13 grupper från olika branscher, från statsförvaltningen till medierna. Den senaste gruppen för informationsutbyte, VESI-ISAC, grundades i höstas. Gruppen för informationsutbyte inom energibranschen, tidigare E-CIP nuvarande E-ISAC, är den grupp som funnits längst. Även 2018 har stora satsningar gjorts för att utveckla gruppernas verksamhet. Kyber 2020-programmet har bidragit med tilläggsresurser för vårt arbete.

I de branschspecifika grupperna är det möjligt att fokusera på just de utmaningar och hot som branschen i fråga står inför. I de olika grupperna har man år 2018 behandlat bland annat valberedskap, skydd mot överbelastningsangrepp, informationssäkerhet i routrar och säkerställande av informationssäkerheten i distansförbindelser till automationsmiljöer samt övat informationsutbyte i störningssituationer.

Även om det finns skillnader inom grupperna, är en stor del av ämnet gemensamt för alla. Bland annat säkerställande av informationssäkerheten i molnbaserade lösningar och frågor gällande personalutbildning är bekymmer som ger gråa hår. På grund av kostnadseffektivitet och en teknologisk miljö som snabbt förändras måste organisationer allt oftare utkontraktera sina informationssäkerhetstjänster. Det krävs specialkompetens för att de utkontrakterade tjänsterna jämte avtal ska fungera.

## Gruppen för informationsutbyte i energibranschen belönades för ett förtjänstfullt samarbete

Energibranschen har ett stort ansvar att trygga samhällets funktion. Sakkunniga i branschen är väl medvetna om detta och samarbetar aktivt för att utveckla cybersäkerheten inom sin bransch. Vi belönade E-ISAC med utmärkelsen Vägvisare för informationssäkerheten för ett exemplariskt samarbete våren 2018.

Under 2018 har man inom i energibranschen betonat vikten av beredskap för problemsituationer, samarbete och utveckling av egna funktioner samt övning av dessa.

I september ordnades övningen TURVA18 vid kärnkraftverket i Olkiluoto. I oktober deltog aktörer i energibranschen och andra företag och myndigheter i övningen TIETO18 om omfattande cybersäkerhetsstörningar. I övningen Black Screen II i november låg fokus på hantering av cyberhot tillsammans med stamnätsbolagen i de nordiska länderna och myndigheterna i branschen. Projektet Kyber-ENE2 bidrog för sin del till att förbättra cybersäkerheten hos branschaktörer som producerar kritiska energiprodukter och -tjänster. Olika workshoppar och övningar om cybersäkerhet kommer också att ordnas under 2019.

Microsoft Office 365-bedrägerierna färgade hela 2018. På sommaren fick vi via våra ISAC-grupper kännedom om otaliga lyckade bedrägerier och flera fall där det var nära ögat. Utifrån uppgifterna bedömde vi situationen i Finland som allvarlig och gick ut med en kritisk varning om bedrägerierna. Varningen hjälpte finländska organisationer att skydda sig mot bedrägerierna och de skador som de föranleder. ISAC-grupperna har även tillhandahållit viktig hjälp och anvisningar för hur man skyddar sig mot Office 365-bedrägerier.

# Nyheter från ISAC-branscherna 2018

| BRANSCH | SÄRDRAG | AKTUELLT |
|---|---|---|
| STATSFÖRVALTNINGEN | Många lagstadgade informationssäkerhetskrav och till följd av internationella skyldigheter. Behov att noga fundera över till exempel frågor i anslutning till geografisk lagring av information. | Flera val ska hållas på våren och på hösten börjar Finlands period som EU:s ordförandeland. |
| FINANS | God beredskap för överbelastningsangrepp som blivit ”det nya normala”. Nätfiskemeddelanden en utmaning för bankerna. | Samarbetet blir mer internationellt och i synnerhet större mellan de nordiska länderna. Uppföljning av införandet av NIS-skyldigheter. |
| VATTENTJÄNSTER | Stort beroende av automationssystem, så skyddet av dessa är ett viktigt föremål för samarbete. | Inledde ISAC-samarbetet 2018. Uppföljning av införandet av NIS-skyldigheter. FBC:s projekt Cyber-Vatten skapade verktyg för att utveckla cybersäkerheten inom vattentjänster. |
| TELEFÖRETAG (ISP) | Lösningar för ett effektivt informationsutbyte om cyberhot såväl när det gäller beredskap för störningssituationer som i operativa störningssituationer. | Samövning för teleoperatörer för beredskap för omfattande störningssituationer. |
| SOCIAL- OCH HÄLSOVÅRD | Metoder för informationssäker delning av patientuppgifter inom hälso- och sjukvården. | FBC:s projekt Cyber-Hälsa utvecklar cybersäkerheten i branschen omfattande. SHM:s beredskapsanvisningar för tjänsteleverantörer inom social- och hälsovården har uppdaterats i fråga om cybersäkerhet. Uppföljning av införandet av NIS-skyldigheter. |
| ENERGI | Omfattande gemensam övningsverksamhet. Beredskap viktig i verksamheten. | Projektet Kyber-ENE2 pågår. Övningar (t.ex. TURVA18 vid kärnkraftverket Olkiluoto, TIETO18, Black Screen II). Uppföljning av införandet av NIS-skyldigheter. |
| KEMI OCH SKOGSINDUSTRI | Verksamheten är beroende av automationssystem och produktionen finns i flera länder. Kräver att informationssäkerhet genomförs i olika arbetskulturer och enligt olika lagstiftning. | Stor ökning av användningen av IoT samt aspekter av utkontraktering. |
| LIVSMEDEL OCH HANDELSDISTRIBUTION | Stor digitalisering av verksamheten, övergår till automatisering och robotisering. | Frågor gällande e-postsäkerhet. |
| TRAFIK | Framtida utmaningar är automatiseringen inom trafiken och en kraftig ökning av nätverksanslutningar. Branschen befinner sig i ett brytningsskede. | ISAC inleder sin verksamhet i början av 2019. Uppföljning av införandet av NIS-skyldigheter. |
| MEDIERNA | Medieorganisationernas produktionssystem ansluts till nätverk. Redaktioners och enskilda redaktörers informationssäkerhet. | Lämpligt skydd av molntjänster. Medieorganisationernas frågor gällande informationssäkerhet i samband med valen. |

# Stöd och planering vid cyberövningar

*”Genom att arbeta tillsammans och nätverka kan man nå framgångar som är större än summan av sina delar.*

# Övningar en möjlighet att lära sig nya saker och öka cyberberedskapen

Målet med övningsverksamheten är att förbättra organisationernas handlings- och återhämtningsförmåga i händelse av allvarliga informationssäkerhetskränkningar. I en övning simuleras en krissituation och genom att lösa den kan deltagarna få värdefulla lärdomar.

Vår övningstjänst är en del av Försörjningsberedskapscentralens projekt Kyber 2020 och finns till för försörjningsberedskapskritiska organisationer. Vi hjälper bland annat till med att hitta en lämplig samarbetspartner, skapa övningsscenarier och välja ett lämpligt övningssätt. Våra tjänster har också använts vid planeringen och utförandet av samövningarna TIETO, KYHA och TAISTO.

## Genom övningar framkommer nyttan med samarbete

Övningen TIETO18 som Försörjningsberedskapscentralen ordnade under hösten förde samman över 120 representanter för företag och myndigheter för att öva att hantera utmanande informationssäkerhetshändelser med hjälp av samarbetsnätverk. Övningen ordnades i tre delar och den sista delen inklusive nedmontering av resultaten tog tre dagar.

För övningen skapades fiktiva organisationer som skulle samarbeta för att bekämpa ett flertal informationssäkerhetshot. Myndigheterna deltog i att lösa problemen och bygga upp handlingsmodeller för att hantera hotsituationerna. YLE, som ordnade en egen beredskapsövning samtidigt, gav övningen en extra krydda. Deltagarna fick ge intervjuer till riktiga reportrar och under den andra övningsdagen sändes även övningsnyheter från platsen.

## Också myndigheterna har nytta av att nätverka

Säkerhetsmyndigheternas egen övning, KYHA, i Jyväskylä ställde myndigheterna inför en verklig utmaning. I övningsmiljön hade man skapat it-system som attackerades av det ”röda lag” som arrangörerna sammanställt.

Även vid KYHA-övningen fokuserade vi på att skapa nätverk för informationsutbyte och en lägesbild utifrån vilken det var möjligt att fatta motiverade beslut vid rätt tidpunkt.

De stora KYHA- och TIETO18-övningarna var bra exempel på cybersamarbete där man genom att arbeta tillsammans och nätverka kan nå framgångar som är större än summan av sina delar.

Samövningarna kompletterar utmärkt företagens och andra organisationers egna övningar där spelsituationerna ofta är begränsade inom de egna fyra väggarna.

Övningar där vi har deltagit i planeringen/genomförandet.

2016: **10** st.
2017: **9** st.
2018: **20** st.

”Cybersäkerhetscentrets agerande i övningarnas centrum var en viktig och framgångsrik del. Satsningen var mycket viktig för övningen.”
– Samövningens arrangör

”I synnerhet i planeringsskedet fick vi bra respons om de realistiska scenarierna och vilka [informationssäkerhetskränkningar] som Cybersäkerhetscentret har sett i verkligheten.”
– En försörjningsberedskapskritisk organisation om sin övning

# Arbetet i framtiden och utveckling av verksamheten

# Med gemensamma krafter skapar vi beredskap för framtiden

Vid vårt verk har vi skapat en expertgrupp som fokuserar på kommunikationsbranschens framtidsutsikter och utveckling. Gruppens syfte är att identifiera nya fenomen och ny teknik i fråga om kommunikation och cybersäkerhet som kommer att förändra vår myndighetsverksamhet, vårt samhälle och vår vardag.

Under år 2018 har gruppen fokuserat på 5G-nät, IoT-apparater för konsumenter och även tagit sikte på bättre informationssäkerhet för molntjänster. Vi har även bekantat oss med 5G- och IoT-ekosystemens verksamhet och satellitteknikens samhälleliga konsekvenser.

## Utredning om 5G-nätens cybersäkerhet

Vi undersökte vilka slags cybersäkerhetsrisker som kan drabba konsumenter, företag och myndigheter när 5G-teknik och kritisk infrastruktur för till exempel företags affärsverksamhet fusioneras i en plattform för datahantering som delas av olika samhällsfunktioner.

Utredningen ger vårt verk vägledning för föregripande och aktuell reglering. På så vis kan aktörer som överväger att införa 5G-teknik skapa trygga lösningar.

Arbetet har framskridit bra och enligt tidtabell, viktiga risker har identifierats och vi känner nu till skillnaderna mellan i synnerhet 5G samt tidigare mobilteknik bättre.

Som nya delområden som kräver särskild uppmärksammet identifierades

**Förmedling av information för hantering:**
Från en infrastruktur koncentrerad kring att förmedla information har man övergått till en infrastruktur koncentrerad kring en komplett datahantering jämte molntjänster. Detta är den största förändringen i 5G-nätet. Informationshanteringen flyttas närmare slutanvändaren och därmed blir även näten mer komplicerade och mer beroende av varandra. Ändringen påverkar traditionella modeller för riskhantering och säkerhetsarkitektur och vi vill delta i utvecklingen av dessa både nationellt och internationellt.

**Operatörerna blir tillhandahållare av en hanteringsplattorm:**
5G-nätets arkitektur utmanar den gamla modellen där en teleoperatör endast förmedlar meddelanden. På grund av 5G-teknikens möjligheter att köra beräkningar och bearbeta data i kanten av nätverket förändras operatörens roll från att endast förmedla meddelanden till att även tillhandahålla en plattform för datahantering. Samtidigt närmar sig nätverkets kärna och kant varandra och teleoperatören får en större roll i tryggandet av slutanvändarnas uppgifter.

**Virtualisering:**
Att tillhandahålla slutanvändare kapacitet för kantberäkningar som grundar sig på virtualisering utmanar teleoperatörer och tillverkare av nätenheter på nya sätt. Nätet går från att vara stängt till mer öppet och större uppmärksamhet måste fästas vid dess informationssäkerhetsuppdateringar. Virtualisering är ett kostnadseffektivt sätt att skala resurser men samtidigt blir det viktigare att identifiera och hantera relaterade risker.

**Sektionering:**
Sektionering av nätet och virtualisering av nätfunktioner gör servicekategorier som erbjuder en bättre prestanda tillgängliga för slutanvändarna. 5G lockar därför även aktörer som tillhandahåller kritiska funktioner att flytta sin nättrafik till mobilnätet. Dessa migrationer kräver en noggrann riskanalys där man även beaktar förändringar i hoten mot den fysiska säkerheten.

I början av 2019 ordnar vi ett 5G-hackathon där vi testar 5G-nätets och IoT-apparaters, som utgör en central del av det, säkerhet och tolerans mot störningar i verkliga användningssituationer. I hackathonet deltar internationella forskare från vårt verks sårbarhetsforskarnätverk.

## Konceptet Informationssäker

Behovet av goda cybersäkerhetsprinciper för IoT-apparater och molntjänster har redan funnits en längre tid. Det har även ansetts viktigt att till exempel konsumenter kan identifiera informationssäkra apparater och tjänster när dessa skaffas.

Med hjälp av konceptet Informationssäker försöker vi möta dessa behov. Konceptet består av frivilliga informationssäkerhetskrav och -principer samt en informationssäkerhetsstämpel. Stämpeln ges till tillverkare som beaktar informationssäkerhet redan i planeringsskedet av sina produkter eller tjänster.

Det övergripande konceptet och principerna finslipas. Dessutom har vi inlett diskussioner med intressenter för att få respons på konceptet och utvecklingsförslag innan det tas i bruk. Samarbetet med tillverkare och återförsäljare av digitala tjänster och IoT-apparater har varit konstruktivt och fört med sig goda idéer för vidareutveckling.

## Utredning om satellitteknik

Vilken är satellitteknikens verkliga roll i samhället? Hur identifieras aktörer med affärsverksamhet i anslutning till satelliter och rymden? Och hur kan man förutse affärsverksamheten i framtiden? Genom vår utredning vill vi få svar på dessa frågor och även fastsälla hur man bäst stöder finländska aktörer. Hur kan man till exempel göra informationssäkerhet till en konkurrensfördel?

Allteftersom satellittekniken blir vanligare kan vi se ingredienser till en teknologisk revolution. Fenomenet kan jämföras med till exempel hur internet blev en del av vår vardag.

Härnäst utreder vi hur man skapar de mest gynnsamma förhållandena för innovationer i samband med informationssäker satellitkommunikation och för ökad affärsverksamhet.

## KYBER 2020 – Programmet för utveckling av cybersäkerhet

Försörjningsberedskapscentralens utvecklingsprogram för cybersäkerhet, KYBER 2020, har haft en central roll i utvecklingen av vår verksamhet ända sedan 2017. Programmets centrala mål är att trygga försörjningsberedskapskritiska företags kontinuerliga verksamhet under alla omständigheter. För att stödja programmet KYBER 2020 har flera utvecklingsprojekt inletts eller kommer att inledas åren 2017–2020.

Verksamheten vid vårt center utvecklas just nu i tre olika projekt, nämligen HAVARO 2.0, ISAC-informationsutbytesgrupperna och övningsverksamheten. Genom projekten vill vi bland annat förbättra vår nationella observationsförmåga, utveckla vår övningsverksamhet och göra informationsutbytet och samarbetet smidigare i våra nätverk. Dessutom deltar vi i utvecklingsprojekt som fokuserar på cybersäkerhetsfrågor i till exempel energibranschen och social- och hälsovårdsområdet.

## HAVARO 2.0 ger bättre skydd mot allvarliga informationssäkerhetshot

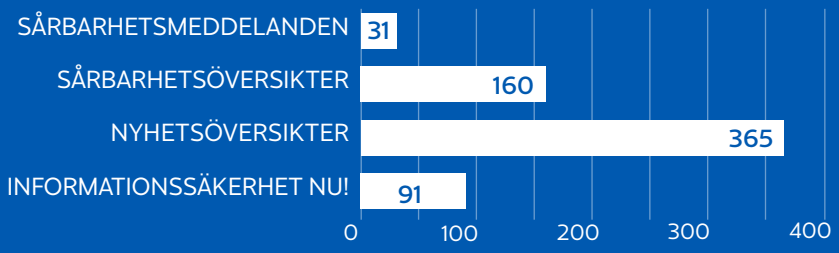
Vår HAVARO-tjänst är avsedd att hjälpa organisationer upptäcka allvarliga informationssäkerhetshot. Just nu håller vi på att ta fram Havaro 2.0 där vi övergår från en myndighetstjänst till en tjänst som produceras av kommersiella aktörer tillsammans med Cybersäkerhetscentret.

Målet med projektet HAVARO 2.0 är att skapa ett förtroendenät där medlemmarna bättre kan byta information sinsemellan än tidigare. Med hjälp av ett snabbt och tillförlitligt informationsutbyte kan HAVARO-tjänsten underhållas och utvecklas så att den motsvarar den kvantitativa och kvalitativa utvecklingen av cyberhot, dock med rimliga resurser. Grunden för verksamheten ska vara Havaro 2.0-systemet och ett avtal om att utveckla programvaran ingicks med Reaktor Oy i september.

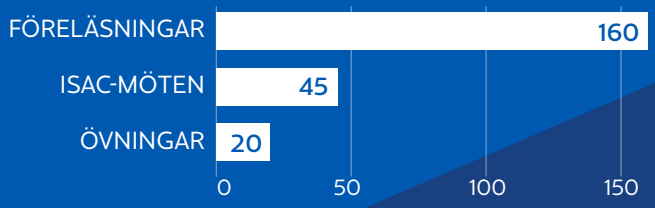
# Nyckeltal för vår verksamhet

I synnerhet vår kommunikation, övningsverksamhet samt branschsamarbete ökade under 2018. Arbetet för att främja cybersäkerheten tar inte slut; till exempel upptäckte systemet Autoreporter betydligt mer trafik från Finland än året innan.

## Kommunikation och meddelanden




## Möten och övningar




OAVBRUTEN JOUR **24/7/365**

VARNINGAR **2**

BEHANDLADE FALL (”TICKETS”) **6100**

ANTAL STÖRNINGAR: ALLVARLIGA **41** BETYDANDE SAMMANLAGT **67**

FALL SOM HANTERATS AV SÅRBARHETSKOORDINERINGEN **35**

STÄNGNINGAR AV SKADLIGA WEBBPLATSER **500**

FÖLJARE PÅ FACEBOOK **5135**

FÖLJARE PÅ TWITTER **8356**

MEDIEKONTAKTER **187**

AUTOREPORTER **154000**

### KUNDERNA ÄR NÖJDA MED VÅRA LÄGESBILDER

Under året genomförde vi tre enkäter om kundnöjdhet där vi tog reda på hur nöjda våra kundorganisationer är med våra lägesbildsprodukter. Bedömningsskalan i enkäten gick från dålig (1) till berömlig (5).

RÄTTIDIGHET: **4,1**

INNEHÅLL: **4,1**

BETYDELSEFULL: **4,1**

### ENKÄT FÖR BRANSCHERNAS INFORMATIONSUTBYTESGRUPPER

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

VITSORD: **4,1**

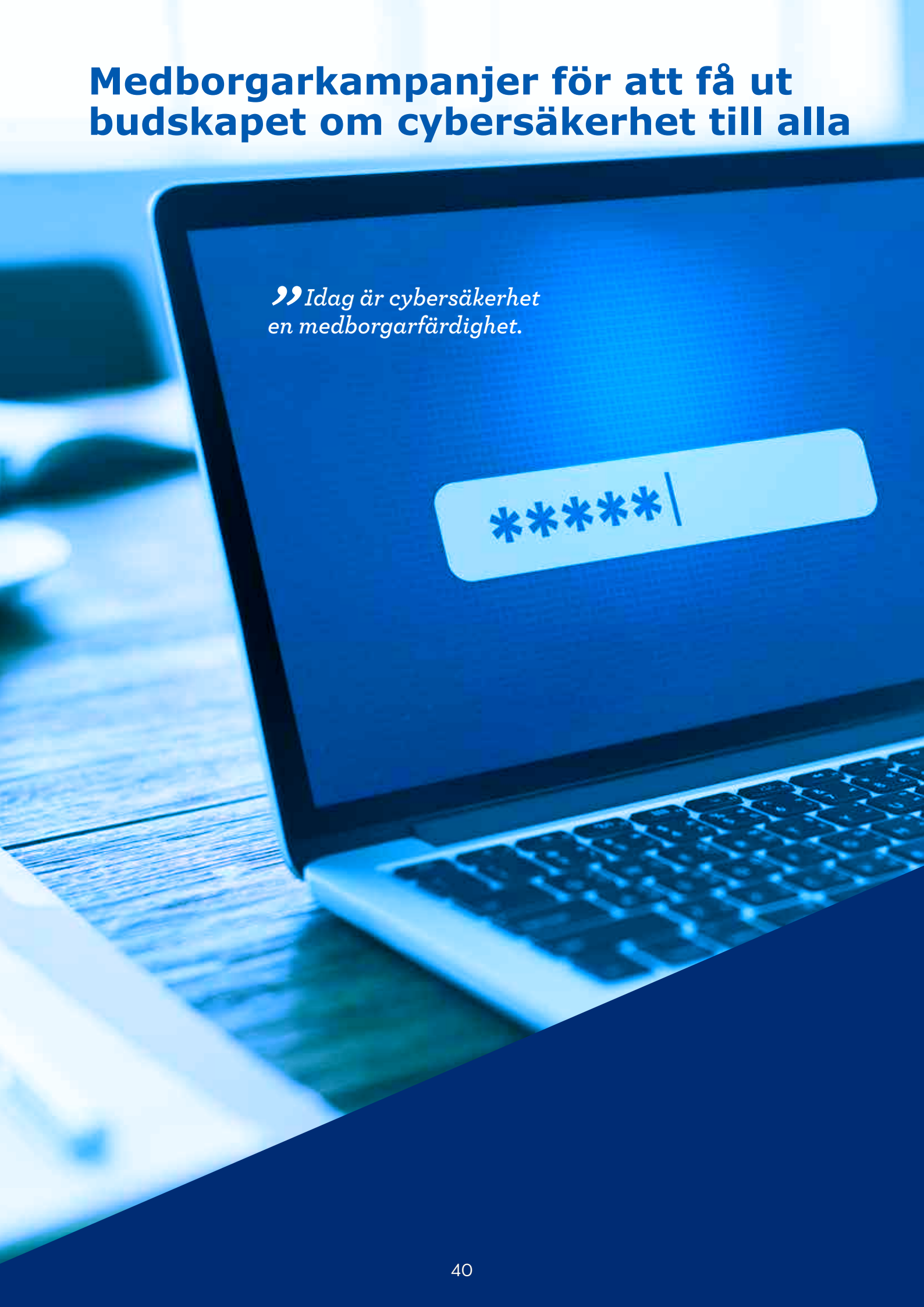
### INTERVJUUNDERSÖKNING FÖR INTRESSENTER

Samordning i anslutning till informationssäkerhetshot och hjälpinsatsens framgång.

VITSORD: **4,2**

Respondenter som använder vår tjänst regelbundet, dvs. varje dag/vecka. **66 %**

# Medborgarkampanjer för att få ut budskapet om cybersäkerhet till alla



*”Idag är cybersäkerhet en medborgarfärdighet.*

## Känner du till lösenords-generatorn Pidempi parempi och Turvalisti-Teijo?

Vi ville nå ut med information om informationssäkerhet till så många som möjligt och gick ut med en kampanj om grundläggande cybersäkerhet i slutet av 2018. Lösenordsgeneratorn Pidempi parempi och Turvalisti-Teijo gav praktiska tips om informationssäkerhet.

Utöver tipsen delade Teijo aforismer om informationssäkerhet till sina följare på kanalen Turvalistit i sociala medier och på webbplatsen turvalistit.fi. Där finns även filmsnuttar med Teijos interventioner för informationssäkerhet.

Vår vardag flyter på när telefoner och datorer fungerar och vi tryggt kan sköta till exempel våra bankärenden på nätet. Myndigheter, elbolag och teleföretag sköter sin del, men var och en av oss bär också ett ansvar. Idag är cybersäkerhet en medborgarfärdighet.


*Lösenordsgeneratorn Pidempiparempi.fi ger dig exempel utifrån vilka du kan skapa dina egna lösenord. Ett bra lösenord ska vara långt och bara du ska känna till det.*



## Kom ihåg dessa grundläggande saker

1. Skapa ett långt och unikt lösenord för varje tjänst du använder.
2. Uppdatera din enhet och dess programvara regelbundet.
3. Säkerhetskopiera viktiga filer och bilder.

# CYBERVÄDRET 2018 OCH EN BLICK MOT CYBERÅRET 2019

# 10 + 1 utsikter för informationssäkerheten 2019

## 1 Den mänskliga aspekten av informationssäkerhet blir större

I takt med att skyddet av informationssäkerheten utvecklas ökar utnyttjandet av människors svagheter allt mer parallellt med tekniska informationssäkerhetshot. Tekniken behövs fortfarande men dessutom behövs skyddslösningar som grundar sig på människors kunnande och beteende.

## 2 Informationssäkerheten hos konsumentprodukter som ansluts till internet blir allt viktigare

Bristfällig informationssäkerhet ställer till förtret såväl för dem som använder IoT-apparater som för andra som sköter ärenden på internet. Genom reglering, internationellt samarbete och standardisering försöker man förbättra situationen. Lyckligtvis är konsumenterna mer intresserade av sina apparaters informationssäkerhet och integritetsskydd. En symbol som anger att en apparat är informationssäker skulle underlätta konsumenternas beslutsfattande.

## 3 Beroendet av digitala tjänster skapar oväntade situationer

Digitaliseringen av tjänster, produkter och processer för med sig stora effektivitetsvinster. Samtidigt föds nya kedjeformade beroenden och den totala riskexponeringen är inte lika synlig. Trycket att genomföra ändringar och försök i affärsverksamheten som bygger på digitalisering är dock stort. Det är ett tufft arbete för riskhanteringen att följa med i förändringarna.

## 4 Kända hot som klassats som ringa blir sakta värre

Kända hot som inte väckt stor uppmärksamhet och som klassats som ringa växer och blir massiva. I synnerhet nätfiske är ett allt mer svårhanterligt gissel och snokandet efter uppgifter blir allt mer riktat. Allt från småkriminella it-brottslingar till statliga aktörer försöker komma åt uppgifter och utnyttja dem. It-brottslingar siktar i synnerhet på ekonomisk vinning och sina offers livsviktiga uppgifter.

## 5 Den nya tekniken bestämmer hur utmaningarna för informationssäkerheten ser ut på 2020-talet

Till exempel är maskininlärning, robotteknik, 5G och artificiell intelligens ny teknik som tas i bruk i en nära framtid. Det investeras också mycket i att utveckla dessa. Hur informationssäkerhet beaktas i utvecklingen och ibruktagandet visar vilka slags informationssäkerhetsutmaningar vi står inför på 2020-talet.

## 6 Molnet är på stadig frammarsch och förändringen gläder och oroar

Informationssäkerhet kräver förmåga att anpassa informationssäkerhet som bygger på traditionella skyddslösningar och molnvärlden till en helhet. Efterfrågan på nytt tänkande och innovativa lösningar växer.

## 7 Allt fler utkontrakterar informationssäkerhet

I synnerhet olika säkerhetsoperationscenter och SOC-tjänster ökar. Även andra externa informationssäkerhetstjänster skaffas allt oftare för att stödja det egna kunnandet.

## 8 Statliga aktörers cyberangrepp och nyhetsrapporteringen om dem fortsätter

Angrepp i cybermiljöer är effektiva och rädslan för att åka fast är liten. Olika länder för fram sina bedömningar av gärningsmännen med ännu större kraft.

## 9 Det finns fortfarande en del att förbättra i organisationers grundläggande informationssäkerhet

Till exempel är man fortfarande inte tillräckligt noga med uppdateringar, säkerhetskopiering och lösenord. I synnerhet i avtal med tjänsteleverantörer och samarbetspartner finns det mycket att förbättra vad gäller informationssäkerheten.

## 10 Informationssäkerhet blir en del av riskhantering som utgår från affärsverksamheten

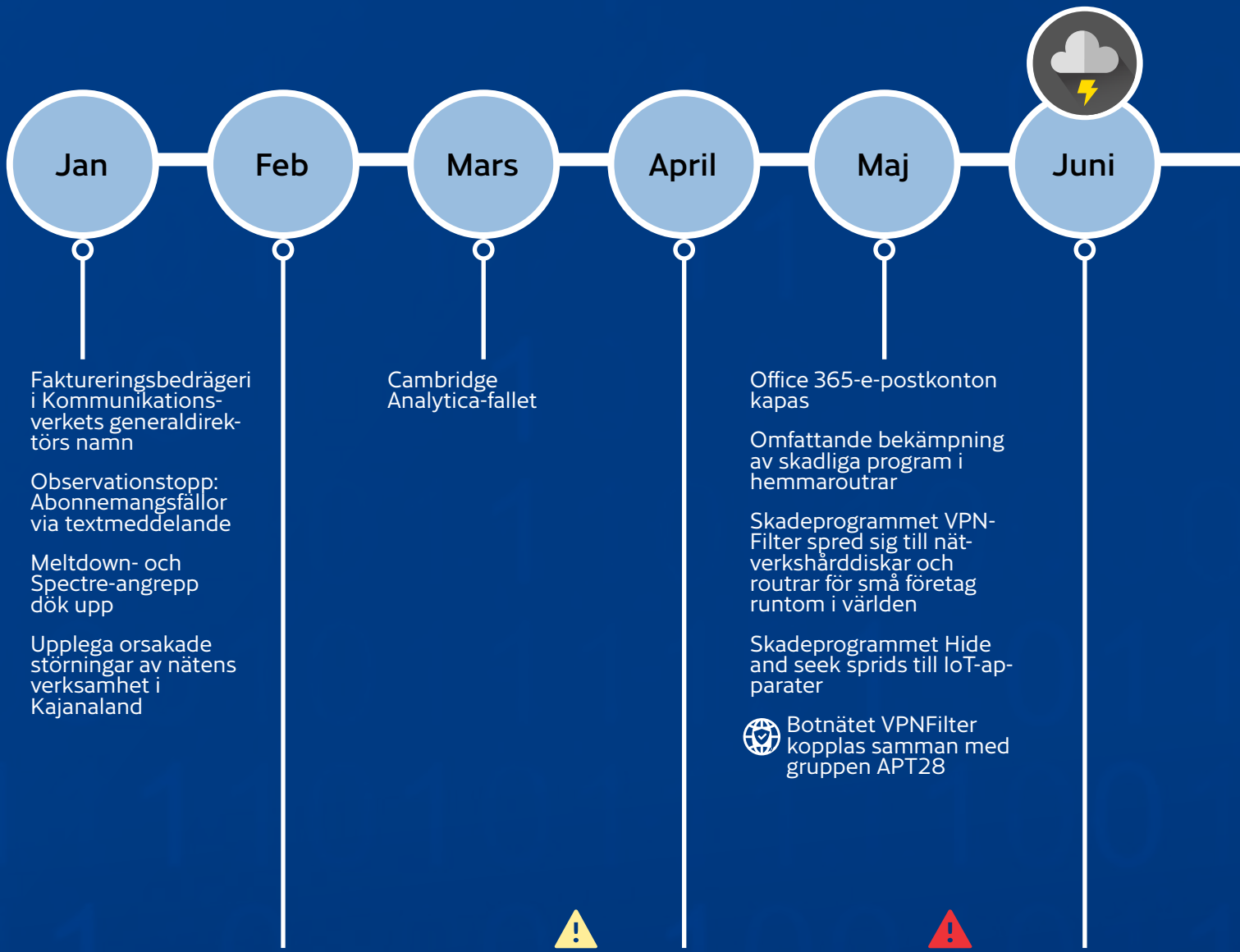
Informationssäkerheten flyttar ut från it-avdelningens skrymslen och kommer upp på organisationernas agenda för övergripande riskhantering. De som fattar beslut om riskerna ska även bära ansvaret för dem. Det är det enda effektiva sättet att bekämpa de ständigt ökande cybersäkerhetshoten.

## +1 Ingen epidemi av skadeprogram riktade mot mobila enheter kommer att ses

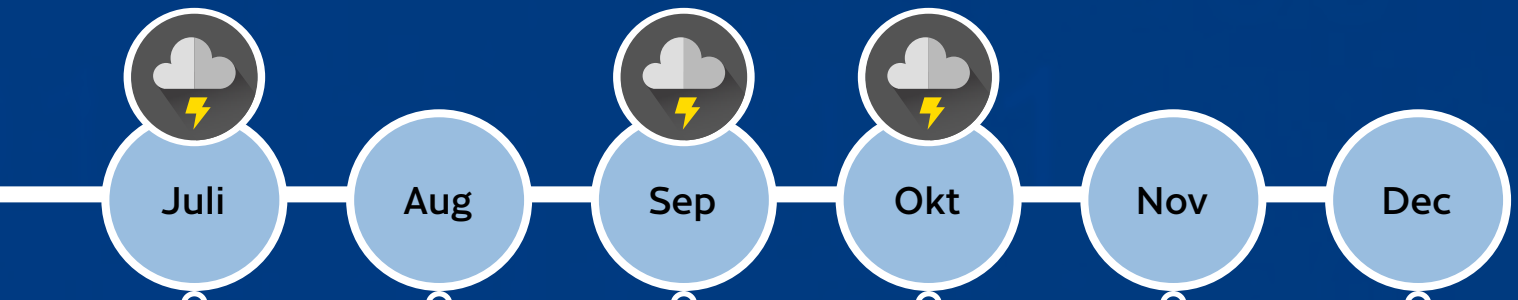
Vi har redan i flera år förutspått en frammarsch för skadeprogram i mobiler, men än så länge har detta inte hänt.

# Cybervädret 2018

## De viktigaste informationssäkerhetsincidenterna januari–december 2018




= Internationell nyhet




**Aktivt nätfiske efter användaruppgifter till Office 365**

Porrutpressningskampanj: Jag vet vad du har för lösenord!

Dataläckor från tillverkare av sportklockor

**Aktivt nätfiske efter användaruppgifter till Office 365, nu även kamouflerade som säkra e-postmeddelanden**

Nätfiske efter betalkortsuppgifter via MinSkatt

suomi.fi utsätts för ännu ett angrepp

Det största överbelastningsangreppet i Finland år 2018 med en volym på 90 Gbit/s

Uppgifter om cirka 50 miljoner Facebook-användare läcker ut

Magecart-angrepp mot nätbutiken Newegg

Misstänkt gärningsman bakom botnätet Satori grips

**Aktivt nätfiske efter användaruppgifter till Office 365**

Marriott utsatt för dataintrång

Dataläcka i appen Yandex

Den tyska informationssäkerhetsmyndighetens (BSI) kriterier för informationssäkerhet i hemmaroutrar

**Nätfiske efter användaruppgifter till Office e-post och kapade konton används fortfarande för bedrägerier**

Överbelastningsangrepp mot nättjänsten Suomi.fi

Magecart-angrepp mot British Airways nätbutik

Sårbarheter i inbyggda program på faxar, även 3D-skrivare är oskyddade på nätet

SÄPO: Försök att påverka riksdagsvalet i Sverige

**Aktivt nätfiske efter användaruppgifter till Office 365**

Finskspråkig version av porrutpressningen

Observationerna av skadeprogrammen Kovter och Emotet ökar

Sårbarheten Port Smash blir känd

Sårbarheter hittas på SSD-diskar

**Aktivt nätfiske efter användaruppgifter till Office 365**

EU:s diplomatkommunikation har utsatts för spionage i många år i form av nätfiske

Amerikansk federal åklagare: APT10-gruppens nätspionage sträcker sig även till Finland

# Utfallet av utsikterna för informationssäkerheten 2018

Våra bedömningar av informationssäkerhetsfenomen under det gångna året träffade ganska bra. Hälften av våra utsikter förverkligades, två gick helt åt skogen och tre klassificerar vi som gränsfall.

## Rätt! Ja

År 2018 fick GDPR och NIS organisationer att satsa på informationssäkerhet. I och med att majoriteten av de infektioner av skadeprogram som vi sett i Finland har berott på oskyddade IoT-apparater som inte uppdaterats, stämde vår prognos om underkända IoT-apparater. Det fanns inte ett för stort utbud av informationssäkerhetskunniga; bug bountyn och hackathons ökade öppenheten och kunskapen om informationssäkerhet. Dessutom utnyttjades utkontrakterade leveranskedjor i dataintrång enligt vår prognos.

## Fel! Nej

Uppdateringskedjor har inte utnyttjas för att sprida skadeprogram på det sätt vi väntade oss. Och bra är väl det. Kriminella har inte heller angripit företag via sociala medier utan använder främst e-post för att sprida bedrägerier och skadeprogram. Kriminellas angrepp på sociala medier drabbar främst privatpersoner.

## På sätt och vis... –

År 2018 blev kombinationen av innovativa informationssäkerhetsprodukter och artificiell intelligens inte ett fenomen, även om man gjorde framsteg i tekniska lösningar och nya lösningar utvecklas hela tiden. Automatik och maskininlärning utnyttjas redan i stor omfattning, tråkigt nog även av it-brottslingar. Dock verkar inte heller kriminella ha utnyttjat artificiell intelligens. Däremot utfördes fler överbelastningsangrepp som fick sin kraft från botnät som består av IoT-apparater. Hackade IoT-apparater användes även för att bryta kryptovaluta. Vi gjorde även observationer om IoT-skadeprogram, men epidemier kunde undvikas.

| | | |
|---|---|---|
| 1 | Ja | **GDPR och NIS får organisationer att satsa på informationssäkerhet** |
| 2 | Ja | **IoT-apparater som dör i nätet är ett problem** |
| 3 | Ja | **Eterfrågan på experter på informationssäkerhet på arbetsmarknaden fortsätter** |
| 4 | – | **Innovativa informationssäkerhetsprodukter utnyttjar artificiell intelligens** |
| 5 | – | **IoT lockar brottslingar och utpressningsprogram** |
| 6 | Ja | **Öppenheten ökar (bug bounty, hackathon)** |
| 7 | – | **Brottslingar effektiviserar sina attacker med hjälp av artificiell intelligens** |
| 8 | Nej | **Uppdateringssäkerheten rubbas** |
| 9 | Ja | **Leveranskedjor som lagts ut på entreprenad utnyttjas vid dataintrång** |
| 10 | Nej | **Sociala medier som en angreppskanal till företag** |

# Sammanställning av nyheter om årets viktigaste händelser

## Bedrägerier och nätfiske

- **Office 365-varning: Aktivt nätfiske efter användaruppgifter till Office 365:**
  https://www.kyberturvallisuuskeskus.fi/sv/natfiske-och-dataintrang-mot-office-365-e-postkonton-mycket-vanliga-upptack-skydda-dig-och
- **Svindlaren håller masken – fakturabedragare uppträder som Kommunikationsverkets generaldirektör:**
  https://legacy.viestintavirasto.fi/sv/cybersakerhet/informationssakerhetnu/2018/01/ttn201801231206.html
- **Porrutpressning:**
  https://legacy.viestintavirasto.fi/sv/cybersakerhet/informationssakerhetnu/2018/07/ttn201807171603.html
  https://www.is.fi/digitoday/tietoturva/art-2000005848028.html
- **Bluff-SMS:**
  https://www.mtvuutiset.fi/artikkeli/poliisi-varoittaa-huijausviesteista-ala-avaa-linkkia-ja-sulje-viesti/6747364#gs.bMJpkrtC
- **MinSkatt:**
  https://legacy.viestintavirasto.fi/sv/cybersakerhet/informationssakerhetnu/2018/09/ttn201809111520.html

## Sårbarheter och skadliga program

- **Meltdown & Spectre:**
  https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2018/01/ttn201801041615.html
- **Wannamine:**
  https://legacy.viestintavirasto.fi/sv/cybersakerhet/informationssakerhetnu/2018/02/ttn201802161123.html
- **VPNFilter:**
  https://legacy.viestintavirasto.fi/sv/cybersakerhet/informationssakerhetnu/2018/05/ttn201805241306.html
  https://www.thedailybeast.com/exclusive-fbi-seizes-control-of-russian-botnet
- **Skadeprogrammet Hide and seek sprids till IoT-apparater:**
  https://www.bleepingcomputer.com/news/security/hide-and-seek-becomes-first-iot-botnet-capable-of-surviving-device-reboots/
- **Kovter, ett skadeprogram som klickar på reklam:**
  https://www.proofpoint.com/us/threat-insight/post/kovter-group-malvertising-campaign-exposes-millions-potential-ad-fraud-malware
- **Banktrojanen Emotet:**
  https://blog.trendmicro.com/trendlabs-security-intelligence/new-malicious-macro-evasion-tactics-exposed-ursnif-spam-mail/
- **Sårbarheten Port Smash:**
  https://www.io-tech.fi/uutinen/intelin-prosessoreista-loytyi-uusi-portsmash-sivukanavahaavoittuvuus/
- **Sårbarheter i SSD-diskar:**
  https://legacy.viestintavirasto.fi/sv/cybersakerhet/informationssakerhetnu/2018/11/ttn201811081513.html

## Dataläckor och -intrång

- **Cambridge Analytica & Facebook:**
  https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election
  https://yle.fi/uutiset/3-10121765
- **Magecart-angrepp**
  – **Ticketmaster:**
  https://www.securityweek.com/ticketmaster-breach-tip-iceberg-major-ongoing-magecart-attacks
  – **British Airways:**
  https://www.bleepingcomputer.com/news/security/british-airways-fell-victim-to-card-scraping-attack/
  – **Newegg:**
  https://www.bleepingcomputer.com/news/security/newegg-credit-card-info-stolen-for-a-month-by-injected-magecart-script/
- **Uppgifter om 50 miljoner Facebook-användare har läckt ut:**
  https://yle.fi/uutiset/3-10430506
  https://legacy.viestintavirasto.fi/sv/cybersakerhet/informationssakerhetnu/2018/10/ttn201810011357.html
- **Sportklockor:**
  https://www.mtvuutiset.fi/artikkeli/viestintavirasto-sijaintitieto-ja-maailmalla-levittaneesta-sovelluksesta-voi-tulla-yllatyksena-etta-tiedot-menevat-kaikille/6987790#gs.kQinniCY
- **Dataintrång hos hotellkedjan Marriott:**
  https://yle.fi/uutiset/3-10534789
- **Dataläcka i appen Yandex:**
  https://www.mtvuutiset.fi/artikkeli/asiantuntija-yandex-kohusta-kyberturvallisuuskeskuksella-ei-ole-resursseja-tutkia-yksittaisten-sovellusten-tietoturvaa/7162778#gs.PZV5cZwA

## Spionage

- **Försök att förstöra OS-arrangörernas it-system:**
  https://blog.talosintelligence.com/2018/02/olympic-destroyer.html
- **Riksdagsvalet i Sverige & cyberpåverkan:**
  https://yle.fi/uutiset/3-10366498
- **Spionage mot den belgiska operatören Belgacom:**
  https://www.theguardian.com/uk-news/2018/oct/25/uk-refusal-cooperate-belgian-hacking-inquiry-condemned-gchq-belgacom
  https://www.theregister.co.uk/2018/10/26/belgium_finds_evidence_gchq_belgacom_hack_proximus/
- **Angrepp via leveranskedjor:**
  https://www.tekniikkatalous.fi/talous_uutiset/yritykset/sahkoposti-harrastuskerhon-vetajalta-kyberrosvot-valmistautuvat-jo-todella-hyvin-keikkoihinsa-pystyy-jopa-tappamaan-6746737

## Överbelastningsangrepp

- **Nedstängning av tjänsten webstresser.org:**
  https://www.bleepingcomputer.com/news/security/europol-shuts-down-worlds-largest-ddos-for-hire-service/
- **Angrepp mot identifieringstjänsten suomi.fi:**
  https://valtori.fi/artikkeli/-/asset_publisher/sunnuntain-12-8-palvelunestohyokkayksen-yksityiskohtia-selvitetaan
  https://yle.fi/uutiset/3-10349357?origin=rss
  https://vrk.fi/artikkeli/-/asset_publisher/suomi-fi-tunnistuksessa-on-kohdistetusta-palvelunestohyokkayksesta-johtuva-hairio
  https://legacy.viestintavirasto.fi/viestintavirasto/blogit/2018/ddosinternetinraksyttavarakkikoiraeisaaaikaanhaavaa.html
- **Memcached, det kraftigaste angreppet i historien (1,7 Tbit/s):**
  https://legacy.viestintavirasto.fi/sv/cybersakerhet/informationssakerhetnu/2018/02/ttn201802281537.html
- **Satori-botnät:**
  https://portswigger.net/daily-swig/hacker-arrested-over-satori-botnet-malware

## Kommunikationsnätens funktion

- **Strömavbrott i Kajanaland:**
  https://twitter.com/CERTFI/status/956127257755635712
  https://erveuutiset.erillisverkot.fi/blog/2018/01/24/sahkot-poikki-kainuussa/
- **Störningar på enskilda nät orsakade avbrott i de viktigaste tjänsterna för samhället:**
  https://yle.fi/uutiset/3-10207164
- **GPS-störningar i Lappland:**
  https://yle.fi/uutiset/3-10498891

## IoT

- **IoT-apparater infekterade med kryptokapare:**
  https://www.bleepingcomputer.com/news/security/prowli-malware-operation-infected-over-40-000-servers-modems-and-iot-devices/
  https://www.fortinet.com/blog/threat-research/pyromineiot--nsa-exploit--monero-xmr--miner----iot-device-scanne.html
- **Faxar och 3D-skrivare:**
  https://blog.checkpoint.com/2018/08/12/faxploit-hp-printer-fax-exploit/
  https://isc.sans.edu/diary/rss/24044
- **Den tyska informationssäkerhetsmyndighetens (BSI) kriterier för informationssäkerhet i hemmaroutrar:**
  https://www.zdnet.com/article/germany-proposes-router-security-guidelines/

TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret

Är du eller din organisation i behov av hjälp för att bekämpa informationssäkerhetskränkningar eller har du frågor om lagstiftningen om cybersäkerhet? Vi utvärderar och godkänner även informationssystem.

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

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

**Följ oss och våra nyheter**
www.kyberturvallisuuskeskus.fi
@CERTFI
www.facebook.com/NCSC_FI

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

KONTAKTUPPGIFTER
Cybersäkerhetscentret
Transport- och kommunikationsverket
Traficom
PB 320
00059 TRAFICOM