Transport- och kommunikationsverket
Cybersäkerhetscentret

Cybersäkerhet och styrelsens ansvar

Traficoms publikationer
2/2020

Innehållsförteckning

Transport- och kommunikationsverket Traficom
Cybersäkerhetscentret

ISBN 978-952-311-465-4
ISSN 2669-8757

Inledning

Företag är allt mer beroende av digitala tjänster och system. Samtidigt ökar cyberhoten mot dessa stadigt. En välkonstruerad cybersäkerhet skyddar företagets funktionsförmåga och säkerställer att företaget i sin affärsverksamhet fullt ut kan dra nytta av de fördelar digital teknologi har att erbjuda. I ett företag är det styrelsens uppgift att främja bolagets intressen. Därför måste styrelsemedlemmarna även ha tillräckliga kunskaper om cybersäkerhet och relaterade affärsverksamhetsrisker.

Guidens syfte

Denna guide ger företagens styrelser verktyg och stöd för att förbättra cybersäkerheten i sina organisationer. Guiden fokuserar inte på teknologi, utan hjälper styrelsemedlemmarna att ställa ledningen och personalen de rätta och kritiska frågorna.

Guiden riktar sig särskilt till styrelsemedlemmar i stora och medelstora organisationer, men den kan även användas som ett dagligt redskap av personer med ansvar för cybersäkerhet. I praktiken kan alla organisationer oavsett storlek och bransch ha nytta av guiden.

Guidens struktur

Guiden innehåller en allmän introduktion till cybersäkerhet. I de olika kapitlen behandlas ett tema ur styrelsens och organisationens synpunkt. Delarna innehåller:

- förklaringar av vilken aspekt av cybersäkerhet det är fråga om och varför man ska ta det på stort allvar
- handlingsmodeller för styrelsen och organisationen
- frågor som styrelsen kan behandla inom organisationen.

Del 1 innehåller en introduktion till cybersäkerhet samt exempel på de vanligaste hoten. Del 2 innehåller anvisningar för kartläggning av nuläget. Del 3, 4 och 5 behandlar riskhantering, förståelse av organisationens hotmiljö samt ansvar och arrangemang för cybersäkerhet. Del 6, 7 och 8 innehåller handlingsmodeller genom vilka styrelsen kan främja upprätthållande och utveckling av cybersäkerheten. Del 9 och 10 tar upp samarbete och planering inför krissituationer.

I slutet av guiden finns bilagor med beskrivningar av den centrala lagstiftningen om cybersäkerhet och myndighetsansvar.

Guiden har skapats av Cybersäkerhetscentret vid Transport- och kommunikationsverket och försörjningsberedskapsorganisationen Digipooli. Utkastet till guiden har kommenterats av Anne Berner, Satu Koskinen, Harri Pynnä, Tuija Soanjärvi och Juhani Strömberg. Guiden grundar sig på NCSC-UK:s publikation Cyber Security Toolkit for Boards.

Mer information och anvisningar om cybersäkerhet finns på Cybersäkerhetscentret vid Transport- och kommunikationsverkets webbplats: https://www.kyberturvallisuuskeskus.fi/sv/

DEL I

Vad är cybersäkerhet?

Cybersäkerhet är fortfarande en relativt ny term utan vedertaget innehåll. I praktiken hänvisar den till nya slags säkerhetsutmaningar till följd av digitaliseringen inom organisationer och samhälle. I den här guiden avses med cybersäkerhet de åtgärder med vilka en organisation skyddar de system, program, enheter och telekommunikationsförbindelser de behöver i sin affärsverksamhet mot cyberhot.

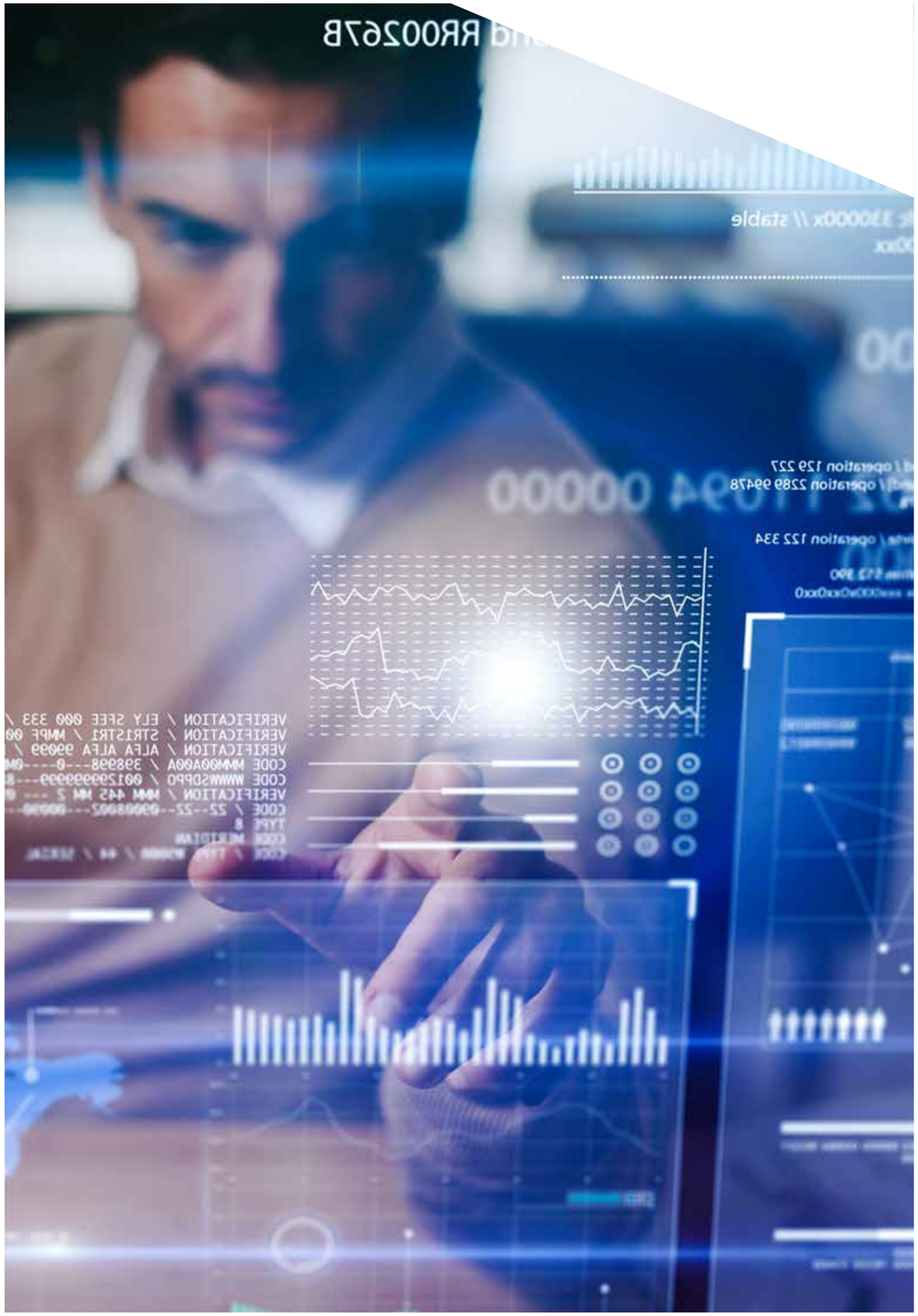
Cyberhot är skadliga händelser eller utvecklingsförlopp som kan påverka organisationens verksamhet, ekonomi, information i dess besittning och i värsta fall rentav affärsverksamhetens fortlevnad.

Exempel på cyberhot

Nätfiske

Syftet med nätfiske (eng. phishing) är för kriminella att komma över kombinationer av användarnamn och lösenord eller annan information som är värdefull för användaren eller organisationen, till exempel betalkortsuppgifter. Till exempel kan den som använder en webbtjänst

Exempel på ett Office 365-bluffmeddelande.



luras att besöka en webbplats som bedragarna skapat och som till sitt utseende påminner om tjänstens riktiga inloggningssida. När användaren matar in uppgifterna på den falska webbplatsen får bedragarna tillgång till dem. Dessa uppgifter kan användas på många sätt beroende på gärningsmännens motiv och vilken roll eller uppgift den användare vars konto man kommit över har i organisationen.

Oftast försöker gärningsmännen lura till sig inloggningsuppgifter till så många e-postkonton som möjligt. Därefter loggar de in på kontona i jakt på sökord med anknytning till fakturering. Dessa uppgifter används för att skapa bluffakturor där man använder samma uppgifter och kontext som en riktig faktura.

Kontot kan även användas för att skicka nya nätfiskemeddelanden till offrets kontakter. Stulna användaruppgifter kan även användas för spionage för att komma över företagshemligheter. Hanteringen av informationen kan även medföra ryktes- och regleringsrisker.

Det är särskilt vanligt med nätfiske via Microsoft Office 365. Det är en mycket populär tjänst i Finland och alla organisationer behärskar inte dess skyddsmekanismer fullt ut ännu.

I Finland har åtminstone flera hundra organisationer fallit offer för nätfiske via Microsoft Office 365. Nätfiskebrott har förorsakat skador som beräknas uppgå till flera miljoner euro.

Som styrelsemedlem har du åtkomst till mycket information som är av intresse för kriminella. Därför kan du själv råka ut för cyberbrottslighet. Angriparna kan till exempel försöka lura till sig dina användarnamn och lösenord till IT-tjänster du använder eller utge sig för att vara du i ett e-postmeddelande. Därefter kan de till exempel skapa och skicka falska e-postmeddelanden för att vilseleda organisationens ekonomiförvaltning att betala bluffakturor.

Exempel 1

Företaget Algol Oy som specialiserat sig på teknisk handel råkade ut för ett skickligt nätfiske via Office 365. En fortfarande okänd gärningsman, vars spår enligt loggdata slutade i Sverige, lyckades bryta sig in i företagets e-postsystem. Därifrån skickade gärningsmannen förfalskade beställningsbekräftelser och betalningsanvisningar som såg trovärdiga ut till ekonomiavdelningen. Resultatet blev en faktura på 140 000 euro som var adresserad till svindlarens bankkonto. Förlusten kunde ha varit ännu större, men till följd av en uppmärksam bank i Hongkong kunde en andra betalning stoppas.

Exempel 2

Med hjälp av nätfiske kunde någon bryta sig in i ett finländskt företag i finansbranschens molntjänst i Office 365. Två av företagets anställda fick ett e-postmeddelande som innehöll en länk till en nätfiskesida. I systemet följde brottslingen företagets e-posttrafik under flera månader och gjorde utan företagets vetskap ändringar i reglerna för vidaresändning av e-post. Företaget hade därför ingen exakt uppfattning om hur länge dess e-posttrafik hade övervakats eller vilken information som kan ha läckt ut från dataföretaget.

Man hade dessutom försökt lägga till fakturor till företagets betalningstrafik. Hade fakturorna betalats hade beloppen överförts till gärningsmännens konton. På fakturan hade information som man kommit över från den normala e-posttrafiken använts och på detta sätt hade man fått fakturan att se så äkta ut som möjligt.

Skadliga program

Skadliga program är datorprogram som orsakar oönskade händelser i IT-systemet eller i delar av det. Vanligen sprider sig skadliga program via bilagor i e-postmeddelanden, webbplatser som infekterats med skadeprogram samt sårbara servrar. Ett skadligt program kan vara nästintill harmlöst, men allt oftare orsakar de också allvarliga problem.

Ett fenomen som också blir allt vanligare runtom i världen är vad som kallas för Big Game Hunting. Termen avser att en gärningsman väljer en särskilt attraktiv och välbemedlad organisation som sitt offer.

Vid angreppet gör gärningsmannen intrång in i organisationens system och vidare till dess nätverk. Till sist startar angriparen ett dolt utpressningsprogram som gör organisationens verksamhet långsammare och skadar den eller lamslår den nästan helt och hållet. Därefter pressas organisationen på pengar för att häva krypteringen. Som namnet anger försöker angriparna hitta föremål med god betalningsförmåga. Också ett stort antal användare eller kunder gör ett föremål attraktivt.

Exempel 3

Cybersäkerhetscentret känner till flera fall i Finland där organisationer som drabbats av utpressningsprogram har råkat ut för stora kostnader till följd av avbrott i affärsverksamheten samt återställande av IT-systemen i funktionsdugligt skick. Åtminstone ett finländskt företag har blivit tvunget att lägga ner sin verksamhet eftersom det skulle ha blivit för dyrt att återuppbygga den IKT-miljö som utpressningsprogrammet förstörde.

Överbelastningsangrepp

Överbelastningsangrepp hör till vardagen på webben och också i Finland sker flera tusen överbelastningsangrepp varje år. I ett överbelastningsangrepp överbelastas nätet med extra datatrafik. Målet är att lamslå en viss tjänst eller ett visst IT-system. Ofta är föremålet för angreppet en organisations offentliga webbplats eller en tjänst som används av till exempel kunder. Vanligen pågår angrepp så länge som de har en inverkan på föremålets verksamhet. Oftast upphör angreppet först när det avvärjts och tjänstens verksamhet har återställts. Många gånger byter angriparen dock bara föremål och fokuserar följande angrepp mot en annan tjänst i samma målorganisation.

Majoriteten av de cyberhot som drabbar en organisation är inte medvetet riktade mot just den organisationen. Till sin natur är cyberbrottslighet mycket opportunistisk. Målet är i det närmaste att hitta svaga punkter i organisationernas system och processer som kan utnyttjas i kriminellt syfte. Verksamheten är ofta internationell och långt automatiserad. Liksom andra brottslingar är cyberbrottslingar intresserade av möjligheten att snabbt komma över pengar.

Majoriteten av de cyberhot som drabbar en organisation är inte medvetet riktade mot just den organisationen.

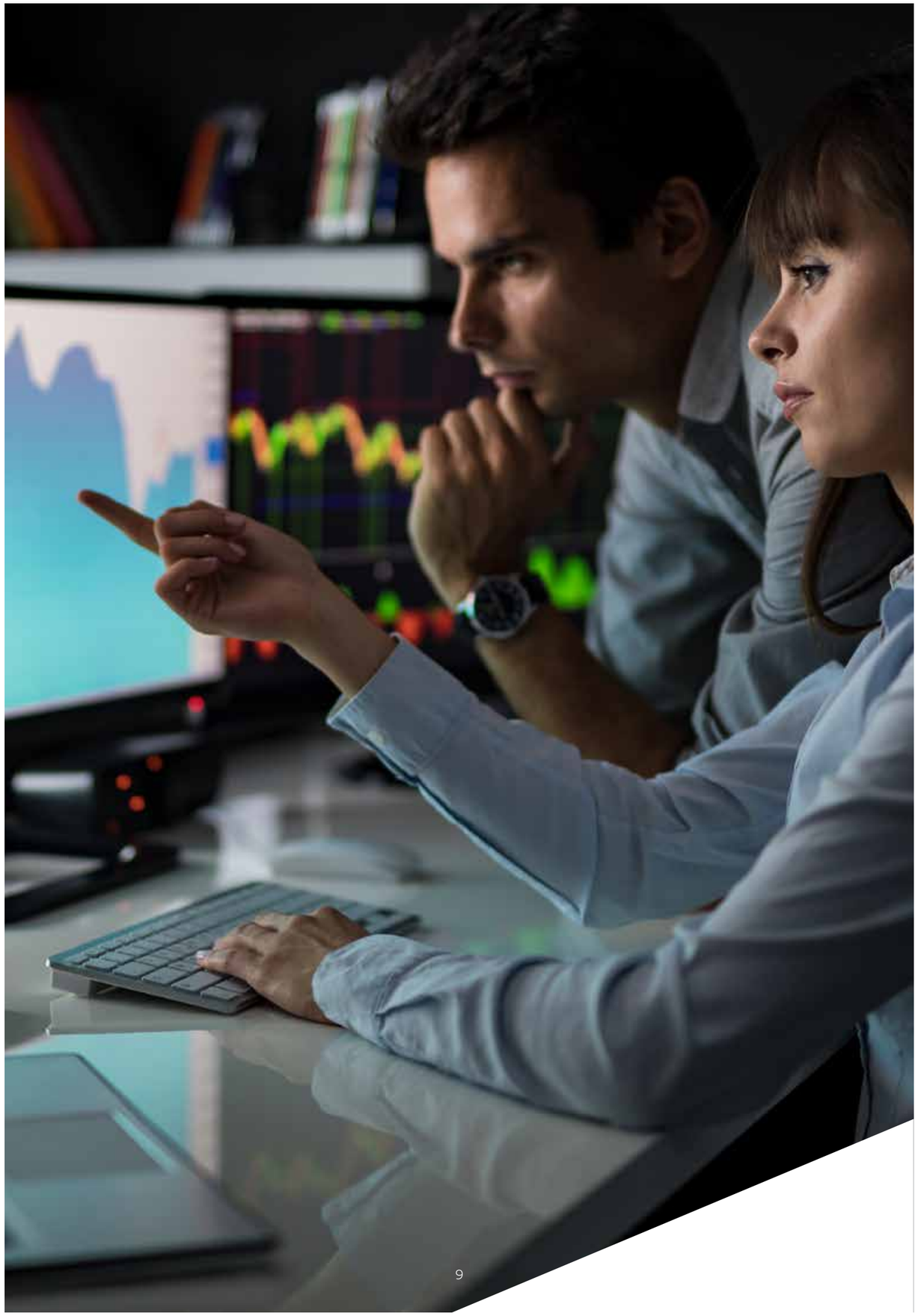
Dessutom genomförs en stor del av cyberangreppen med mycket enkla medel, bland annat olika slags bluffmeddelanden med hjälp av vilka man försöker samla in till exempel användarnamn och lösenord till användare inom en organisation. Därför kan man också förbättra cybersäkerheten med enkla medel, till exempel genom att utbilda personalen att känna igen svindleriförsök.

Organisationen måste utveckla cybersäkerheten följdriktigt och rikscentrerat. De åtgärder som behövs kan vara såväl tekniska som icke-tekniska till sin natur. Det är styrelsens uppgift att sörja för att organisationen besitter tillräckliga kunskaper om cybersäkerhet. Ledningen å sin sida ska ha nödvändig information för att kunna fatta korrekta och effektiva beslut.

Exempel 4

De flesta överbelastningsangreppen på internet består av normal trafik och det är endast föremålet för angreppet som med säkerhet kan bedöma huruvida det är fråga om ett angrepp. Överbelastningsangrepp kan inte förhindras helt och hållet. Därför är det viktigt att organisationer förbereder sig på att uthärda dem och kommer överens med sina internetleverantörer om hur dessa angrepp ska bekämpas. Man kan även bli ett sidooffer för ett överbelastningsangrepp, om angreppet riktar sig till exempel mot det serverhotell som organisationen använder.

Flera organisationer råkar ut för överbelastningsangrepp varje dag i Finland och dessa ska också beaktas i riskbedömningen. Om företagets tjänster måste vara tillgängliga på nätet hela tiden, ska man också planera hur man skyddar sig mot överbelastningsangrepp. Dessutom måste man förbereda sig på dem i god tid.



DEL II

Organisationens utredning av situationen

Inom organisationen ska man ta reda på vilka delar av den informationstekniska miljön (system, data, tjänster och nätverk) som är mest kritiska för att organisationen ska kunna uppnå sina mål. Dessutom måste organisationen förstå vad dess informationstekniska miljö består av i praktiken.

I organisationen ska man specificera vilka delar av den informationstekniska miljön som är kritiska för att uppnå affärsverksamhetsmålen.

Vad kan styrelsen göra?

Ta reda på det viktigaste

Liksom andra risker i affärsverksamheten kan en organisation aldrig avlägsna alla cybersäkerhetsrisker. Styrelsen ska dock säkerställa att man i organisationen skyddar i synnerhet sådant som stöder uppnåendet av målen för affärsverksamheten.

Styrelsen ska övergripande överväga risker. Styrelsen och ledningen kan till exempel veta att en viss samarbetspartner är av avgörande betydelse för organisationen och att det vore katastrofalt för organisationens ekonomi och rykte om denna partners information äventyrades. Också de som ansvarar för organisationens cybersäkerhet ska alltid informeras om dessa risker.

Kommunikationen mellan styrelsen, ledningen och sakkunniga ska vara aktiv och kontinuerlig eftersom styrelsen och ledningen har information om affärsverksamheten som tekniska sakkunniga inte nödvändigtvis har. Denna information är till exempel vilka samarbetsrelationer organisationen prioriterar. Tekniska sakkunniga däremot har information om förutsättningarna för att uppnå de centrala målen. Denna information är till exempel vilka system eller data som samarbetspartners är beroende av.

De viktigaste affärsverksamhetsfaktorerna är de som är mest värdefulla för organisationen. De kan vara värdefulla helt enkelt för att organisationen inte kan fungera utan dem. Äventyrande av affärsverksamhetsfaktorerna kan skada organisationens rykte eller leda till ekonomiska förluster. De kan till exempel vara:

- personuppgifter som organisationen innehar
- organisationens immateriella rättigheter
- en offentlig webbplats
- styrsystem för industri
- system för hantering av användare och åtkomst till internt nätverk.

Vad kan man göra inom organisationen?

Definition av utgångsläget

Det är viktigt att definiera utgångsläget eftersom det ger en bild av vilka skyddsåtgärder som organisationen behöver och som över huvud taget är möjliga. När man fastställer skyddsåtgärderna är det av avgörande betydelse att man känner till

- vilka system som är anslutna till varandra
- vem som har åtkomst till vissa data
- vem som äger vilket nätverk eller vilken tjänst.

Att samla in denna information gör det bland annat möjligt att uppdatera sårbarheter i systemen och skydda sig från angrepp. Informationen kan också behövas när man reagerar på ett angrepp för att man ska kunna bedöma hurudana skador angriparen kan åstadkomma eller vilken inverkan eventuella avhjälpande åtgärder har.

Att skapa en komplett uppfattning av miljön kan vara en svår uppgift, i synnerhet i organisationer vars nätverk och system har växt organiskt med tiden. Men redan att förstå grundläggande saker, såsom vilka system som finns i organisationens olika nätverk, är till hjälp när nödvändiga åtgärder ska sättas in.

Definition av kritiska informationstekniska resurser

I organisationen ska man definiera vilka delar av den informationstekniska miljön som är viktigast för att uppnå affärsverksamhetsmålen. För en organisation kan det till exempel vara viktigt att vara mån om långvariga kunder. Med hjälp av cybersäkerhetsåtgärder kan man stödja förverkligandet av detta mål till exempel genom att skydda kunduppgifter, genom att säkerställa att beställnings-leveranssystemet fungerar utan störningar samt genom att säkerställa att organisationens webbplats fungerar i alla situationer.

Samarbete med tjänsteleverantörer och samarbetspartners

De flesta organisationer har tjänsteleverantörer eller samarbetspartners av vilka de får, med vilka de delar eller till vilka de tillhandahåller information, system eller tjänster. Organisationen ska beakta dessa utomstående tjänsteleverantörer och samarbetspartners i sin riskhantering. Ett centralt sätt är att avtala om ansvar och rättigheter i anslutning till cybersäkerhet med samarbetspartnerna.

Att fundera på

Förstår vi som organisation hur de tekniska systemen, processerna eller resurserna främjar uppnåendet av våra mål?

- Vilka informationstekniska resurser är kritiska för vår organisation och skulle vi inte klara oss utan dem?
- Vilka krav måste vi uppfylla (t.ex. juridiska krav eller avtalade skyldigheter)?
- Vad vill vi inte att ska hända och hur skulle det kunna hända?
- Har vår organisation en process för att identifiera viktiga system, information och tjänster samt för att följa upp funktion och informationssäkerhet i fråga om dessa?

Har kommunikationen om organisationens viktigaste mål varit tydlig inom organisationen och har det säkerställts att dessa prioriteringar också styr cybersäkerhetsåtgärderna?

- Cybersäkerheten ska stödja organisationens strategi. Dokument som styr cybersäkerheten, såsom cybersäkerhetsstrategin eller -policyn, ska skydda organisationens strategiska mål.

DEL III

Riskhantering och cybersäkerhet

Organisationer gör ofta riskbedömningar endast för att överensstämma med krav. Dessa kan till exempel vara:

- yttre faktorer, såsom skyldigheter till följd av regleringskrav
- kundernas krav
- lagstadgade krav.

Om risker endast bedöms av dessa anledningar, är det risk att riskhanteringen bara blir något man bockar av. I en sådan situation kan organisationerna tro att de har riskerna under kontroll fast de endast har följt en fastställd process.

Att följa kraven är inte det samma som säkerhet. De kan överlappa varandra, men i praktiken kan man följa allmänna säkerhetskrav med dålig säkerhetspraxis. God riskhantering går längre än att enbart följa kraven.

God riskhantering går längre än att enbart följa kraven.

Vad kan styrelsen göra?

Inkludera cybersäkerhet i organisationens riskhanteringsprocesser

Cyberrisker ska vara en del av organisationens dagliga riskhantering. Att behandla cyberrisker separat eller enkelt klassificera dem som ”informationstekniska risker” gör det svårare att identifiera deras konsekvenser. Samtidigt kan det även bli oklart hur organisationens övriga risker kan påverka dess cybersäkerhet.

Cybersäkerhetsåtgärderna ska stödja och möjliggöra affärsverksamheten genom att hålla riskerna med digital teknologi under kontroll. Dock får de inte hindra eller försvåra väsentliga åtgärder som främjar affärsverksamheten eller leda till orimliga kostnader.

Mät inte framgångar med hur mycket risknivån minskar

Det kan också vara svårt att mäta huruvida åtgärderna har varit framgångsrika. Ett typiskt slutresultat när cybersäkerheten är på en bra nivå är att verksamheten löper utan störningar. Detta kan dock vara svårt att mäta eftersom störningar även kan bero på sådant som inte har samband med organisationens cybersäkerhetsåtgärder.

I riskbedömningar vill man vanligtvis sätta ett värde på riskens sannolikhet och effekter (till exempel stor – medelstor – liten). Det kan vara lockande att använda en sådan bedömningsmetod för att mäta åtgärdernas framgång. Det är dock skäl att beakta att sådana bedömningar kan vara bristfälliga när det gäller att mäta åtgärder som organisationen vidtagit. Detta beror på att yttre faktorer som påverkar cyberrisker, såsom sårbarheter i programvara, förändras snabbt och ofta är bortom en organisations påverkansmöjligheter.

Exempel på hur man mäter åtgärder finns nedan i avsnittet VIII ’Genomför nödvändiga åtgärder’.

Vad kan man göra inom organisationen?

Samma riskhanteringsprinciper som tillämpas på andra risker tillämpas även på hanteringen av cyberrisker. Cybersäkerhetslösningar och teknologin utvecklas dock så snabbt att det finns en risk att man hamnar på efterkälken och använder föråldrade metoder för att bedöma cyberrisker. Därför är det bra att bedöma cyberrisker oftare än andra risker.

Cybersäkerhet är fortfarande en ny term och användningen av den har ännu inte etablerats. Därför har organisationen inte nödvändigtvis samma förståelse för cyberrisker som till exempel för ekonomiska risker eller risker i anslutning till arbetstagarnas säkerhet. Det finns inte heller nödvändigtvis något kunskapsunderlag att bedöma riskerna utifrån. Det är bra att beakta detta när man funderar kring hur tillförlitlig en cyberriskbedömning är – i synnerhet om resultaten från bedömningen jämförs direkt med ”traditionella” riskbedömningar.

Att fundera på

Har organisationen en process för att säkerställa att beslutsfattarna får så heltäckande information som möjligt?

- I processen ska man i första hand fokusera på att beslutsfattarna kan fatta beslut utifrån bästa möjliga tillgängliga information. Beslutsfattarna kan vara styrelsen, ledningen eller övriga arbetstagare i organisationen. Såväl styrelsen som den som genomför åtgärden ska få tillgång till så mycket begriplig information som möjligt som stöd i besluts-fattandet.
- Därför måste resultaten av riskbedömningarna struktureras enligt deras betydelse. Oftast är kvalitativa resultat ett bättre alternativ än resultat till vilka man lägger till godtyckliga siffror eller koefficienter för att få ett poängvärde.

Har organisationen en process där bedömningen av cyberrisker har inkorporerats i bedömningen av affärsverksamhetens risker?

- Bedöms cyberrisker som en del av affärsverksamhets- och andra beslut?

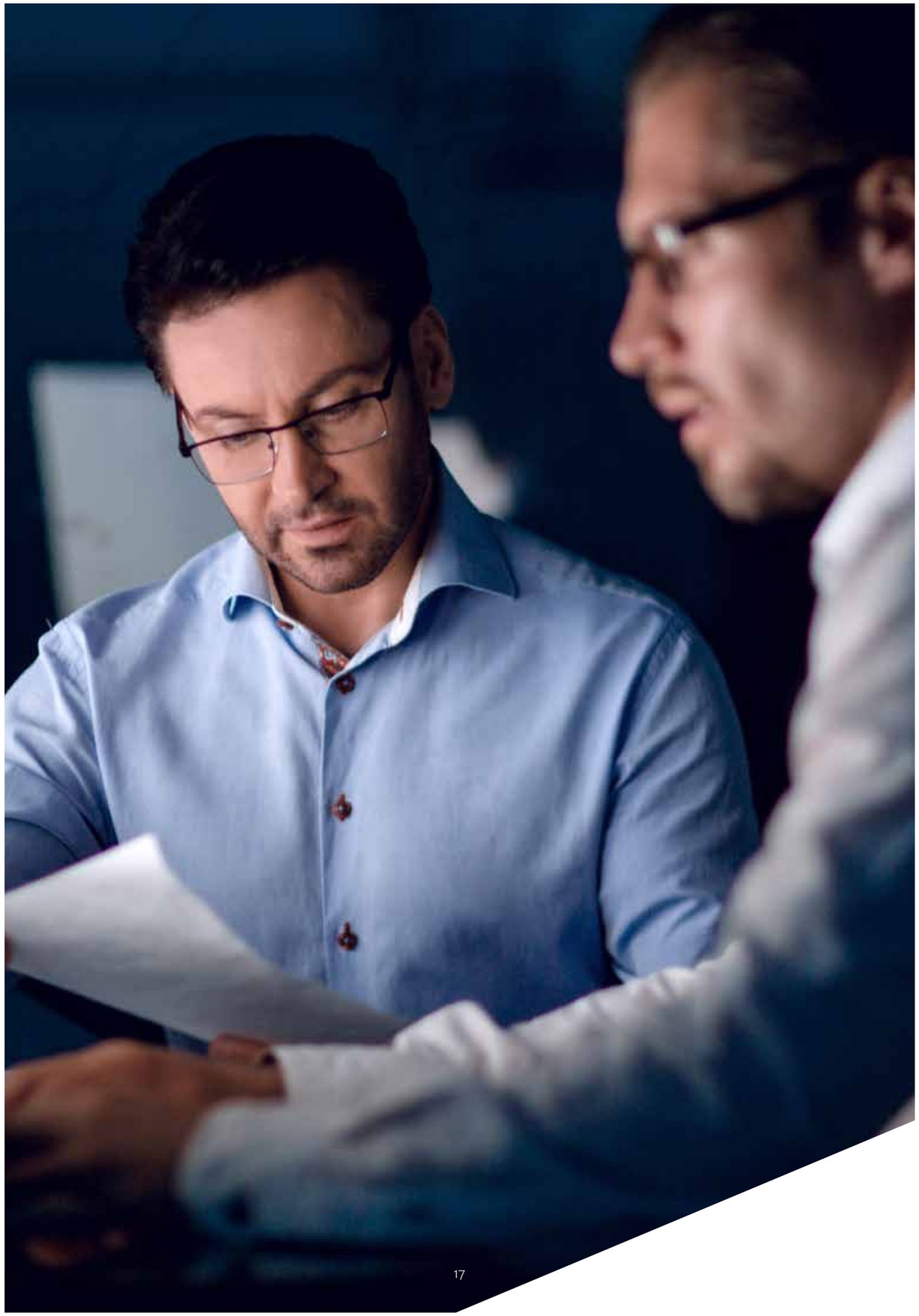
Har organisationen ett effektivt och ändamålsenligt angreppssätt för hantering av cyberrisker?

Styrelsen och övriga aktörer inom organisationen ska kunna demonstrera processen tydligt och enkelt på ett par minuter till exempel med hjälp av följande information:

- Hur eskaleras riskerna?
- Var går tröskeln för styrelsens deltagande i ett riskbeslut?
- Hur ofta bedöms riskerna?
- Vem ansvarar för vilken risk?
- Vem ansvarar för riskbedömningsprocessen och att den är ändamålsenlig?

Har styrelsen och ledningen tydligt definierat hur riskerna ska hanteras inom organisationen?

- Är processerna för rapportering om risker tydliga?
- Har olika risker bedömts sinsemellan? Har betydelsen av olika risker kommunicerats inom organisationen? En risk som organisationen kan godkänna är till exempel att e-posten inte fungerar under en dag, men inte att personuppgifter läcker ut i offentlighe-ten från organisationen.
- Har anhopning av risker beaktats? Hur går man till väga inom organisationen om två eller flera risker inträffar samtidigt?



DEL IV

Vad hotar vår organisation?

När man förstår hoten mot en organisation eller dess samarbetspartners kan man också definiera organisationens cybersäkerhetsåtgärder och -investeringar. Inom organisationen ska man fatta ett medvetet beslut om mot vilka hot organisationen försöker skydda sig. I annat fall är risken att man försöker skydda sig mot allt, vilket lätt leder till ineffektiva åtgärder.

Vad kan styrelsen göra?

Förstå hotet

Att förstå cyberhoten hjälper styrelsen att fatta medvetna beslut som styr verksamheten. Kännedom om angriparnas motiv är centralt: Varför är de intresserade av just er organisation? Angriparens motiv kan givetvis vara endast det faktum att er organisation har internetanslutna datorer med identifierade sårbarheter som kan utnyttjas för kriminell verksamhet.

Säkerställ att organisationen bedriver ett säkerhetssamarbete

Samarbetspartners och referensorganisationer är ofta bra källor för information om hot och god skyddspraxis. Att utveckla samarbetsrelationerna och informationsutbytet kan hjälpa att märkbart förbättra förmågan att skydda sig mot cyberhot. Detta ska inte heller ses som en konkurrensrisk: i slutändan vinner alla på att dela information.

Utvärdera hoten

Kartläggning av betydande hot och potentiella angripare gör det lättare att fatta beslut om mot vilka hot organisationen aktivt bör skydda sig.

En kontinuerlig diskussion mellan organisationens ledning, styrelse och sakkunniga hjälper organisationen att prioritera hot och nödvändiga skyddsåtgärder. Sakkunniga förstår hotens tekniska natur. Styrelsen å sin sida förstår varför organisationen kan vara attraktiv för angripare. Det är dessutom viktigt att redan på förhand diskutera alla beslut som kan ha en betydande inverkan på organisationens hotprofil. På så sätt har tekniska sakkunniga tillräckligt med tid för att genomföra nödvändiga skyddsåtgärder.

Cybersäkerhetscentret uppmanar alla organisationer till aktivt informationsutbyte. Cybersäkerhetscentret driver branschspecifika ISAC-grupper för informationsutbyte (Information Sharing and Analysis Centre). Säkerställ att organisationen deltar aktivt i informationsutbyte om cybersäkerhet till exempel som en del av branschens ISAC-grupp eller något annat informationsutbyte. Mer information om ISAC-verksamheten: https://www.kyberturvallisuuskeskus.fi/sv/vara-tjanster/lagesbild-och-natverksledarskap/isac-grupper-utbyte-av-information

Vad kan man göra inom organisationen?

Underskatta inte oriktade angrepp

I ett oriktat angrepp vill angriparen nå tusentals potentiella offer samtidigt istället för ett specifikt utvalt offer. Angriparna använder ofta automatiska verktyg som är allmänt tillgängliga och som till exempel skannar offentliga webbplatser eller andra tjänster i jakt på sårbara system eller tjänster. När sådana har hittats utnyttjar samma verktyg automatiskt sårbarheten till exempel för att genomföra ett dataintrång. Konsekvenserna av ett sådant massangrepp kan vara lika allvarliga som av ett riktat angrepp. En god grundläggande cybersäkerhetsnivå däremot skyddar systemen från merparten av dessa oriktade angrepp.

Skaffa god lägesbildsinformation och använd den

För beslut som styr verksamheten behövs lägesbildsinformation om cybersäkerheten. Det finns många aktörer på marknaden som erbjuder denna information. Innehållet i informationen kan variera från årsberättelser om allmänna trender till tekniska rapporter om vissa typer av skadeprogram. I Finland producerar bland annat Cybersäkerhetscentret en lägesbild om cybersäkerhet: https://www.kyberturvallisuuskeskus.fi/sv/

Att fundera på

Vilka hot är av betydelse för organisationen och varför?

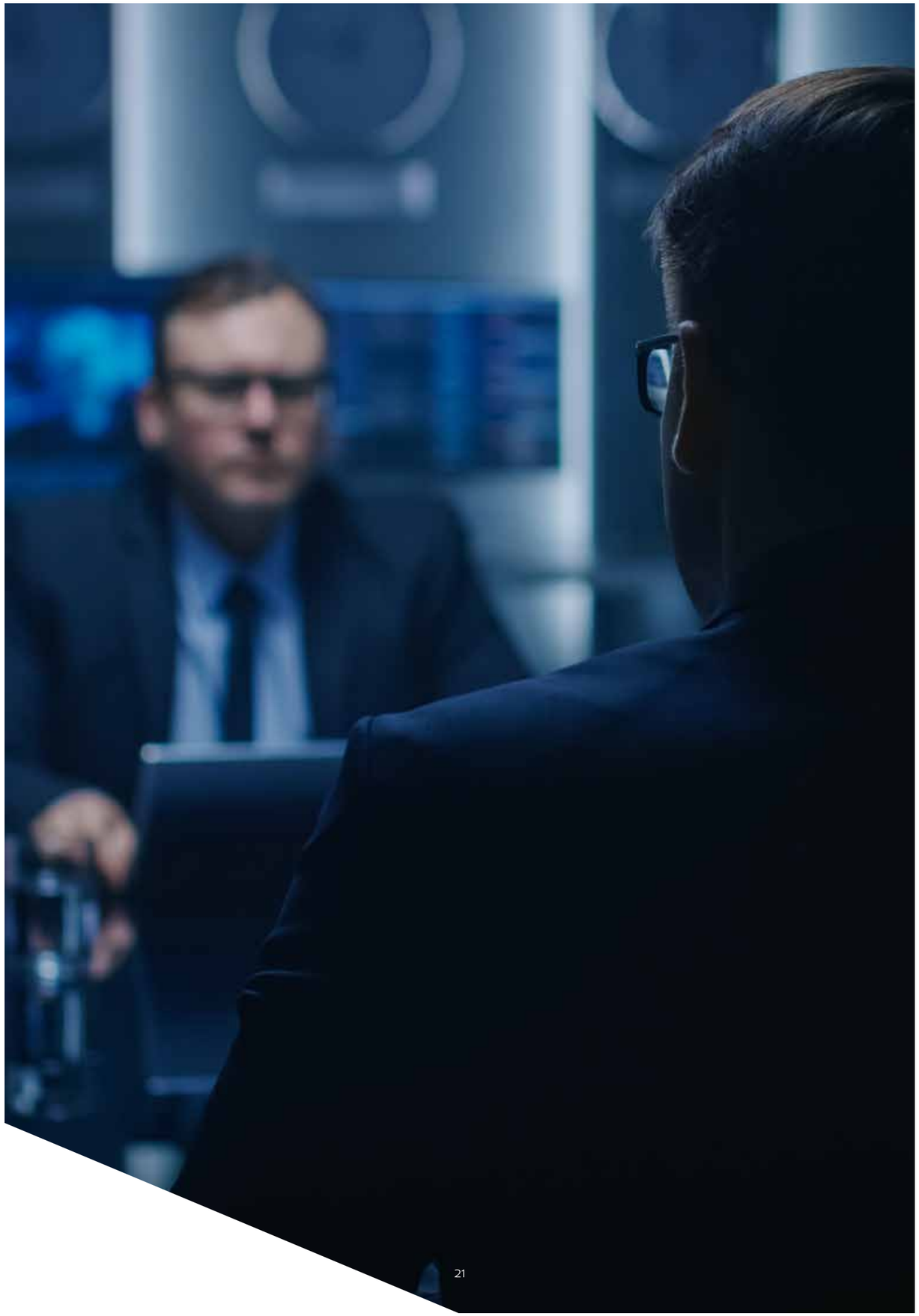
I bedömningen:

- definieras hotens potentiella konsekvenser och sannolikheten för att hoten är riktade mot organisationen
- definieras vilka slags risker organisationen är redo att uthärda
- utnyttjas material om angrepp som organisationen utsatts för tidigare.

Hur håller sig vår organisation uppdaterad om cyberhot?

Organisationen kan:

- söka bevis på angrepp i sina eventuella systemloggar
- utnyttja olika lägesbildsprodukter (till exempel Cybersäkerhetscentrets lägesbilds produkter)
- delta i informationsutbyte (till exempel i ISAC-gruppen för informationsutbyte)
- införa sätt för att internt dela information om centrala cyberhot.



DEL V

Cybersäkerhet som en del av organisationens mål

Cybersäkerhet är ett viktigt element i genomförandet av organisationens mål och den ses allt oftare även som en konkurrensfaktor. Detta förutsätter en positiv cybersäkerhetskultur, investeringar i cybersäkerhet och en korrekt hantering av cybersäkerhet inom organisationen.

Vad kan styrelsen göra?

Cybersäkerhet är en del av organisationens mål och risker

Cybersäkerhet har en övergripande inverkan på organisationen. Därför ska cybersäkerhet inkorporeras i organisationens riskhantering och beslutsfattande så att den kan hanteras på rätt sätt. Till exempel:

- Cybersäkerheten påverkar sannolikt de operativa riskerna eftersom organisationen är beroende av att de många digitala tjänsterna är säkra (e-posttjänster, programvara, etc.).
- En cyberrisk är förbunden med juridiska risker såsom avtalade krav på att skydda affärskompanjoners information och lagstadgade krav på särskilda sätt att han tera uppgifter.
- Cyberrisker kan vara ekonomiska risker, till exempel förlust av tillgångar i nätsvindlerie eller avbrott i tjänsteutbudet till följd av ett cyberangrepp.
- När cybersäkerheten är på en bra nivå kan organisationen ta planenliga risker och utnyttja ny teknologi fullt ut.

Cybersäkerheten bör vara inbyggd i organisationens verksamhet. En bra cybersäkerhetsnivå förutsätter förutom fungerande teknologi även att hela personalen är förtrogen med informationssäkerhetspraxis och har förbundit sig till den.

Organisationen kan till exempel förhindra angripare från att komma över känslig information och säkerställa att åtkomsten till denna information endast innehas av personer som har ett aktuellt och verifierat behov av att få ta del av informationen. Organisationen ska då säkerställa att:

- Den tekniska förvaringslösningen för informationen är ändamålsenlig.
- Den personal som hanterar informatio nen erbjuds utbildning om detta.

Vad kan man göra inom organisationen?

Cybersäkerhet påverkar hela organisationen – inte enbart IT-förvaltningen. Därför får allt ansvar inte läggas på en och samma person inom organisationen. Lyckade cyberangrepp kan till exempel påverka nätförsäljningen och avtalsrelationer eller leda till rättsliga eller regleringsåtgärder. I styrelsen ska det också finnas tillräcklig sakkunskap så att den kan styra organisationens cybersäkerhet.

Involvera sakkunniga

Fundera om styrelsen får den information den behöver om organisationens cybersäkerhet. Det är viktigt att den som ansvarar för cybersäkerheten inom organisationen har en fungerande länk till organisationens ledning och att rapporteringen om cybersäkerhet har ordnats på ett fungerande sätt.

Att fundera på

Förstår vi hur cybersäkerheten påverkar styrelsens och ledningens ansvar? Fundera på följande:

- Har styrelsen tillräcklig sakkunskap för att förstå cybersäkerhetens betydelse för organisationens affärsverksamhet och strategiska mål?
- Vem ansvarar för att övervaka cybersäkerheten?
- Har vi klart och tydligt kommunicerat vilken information om cybersäkerhet som styrelsen och ledningen behöver?

Vem ansvarar för cybersäkerheten just nu? Ansvaret ska ligga hos en namngiven person. Fundera på följande:

- Hur kontaktar han eller hon styrelsen? Rapporterar han eller hon direkt till styrelsen eller deltar han eller hon i någon annan rapporteringsprocess? Uppmuntrar han eller hon styrelsen att aktivt delta i diskussioner om cybersäkerhet?
- Vilka är hans eller hennes mål och vem fastställer dem? Främjar dessa mål cybersäkerheten på ett sätt som gagnar hela organisationen?
- Är han eller hon i kontakt med alla nödvändiga personer för att säkerställa en effektiv cybersäkerhet? I sin allra enklaste form kan detta innebära att personalresurserna inom cybersäkerheten är tillräckliga. Det kan även innebära andra delområden inom organisationen såsom personalförvaltning och ekonomiförvaltning.

På vilket sätt säkerställer vi i styrelsen att organisationens cybersäkerhetsåtgärder är effektiva? Styrelsen bör säkerställa att:

- Organisationen har lämpliga tekniska skyddslösningar till sitt förfogande och att styrelsen informeras om resultatet av dessa på ett begripligt sätt.
- Hotbedömningar och nödvändiga skyddslösningar granskas regelbundet och skyddsåtgärderna uppdateras därefter.

Har vår organisation en process för att säkerställa att cyberrisker har inkluderats i affärsverksamhetens risker?

- Har organisationen en process för att bedöma risker och konsekvenser av olika funktioner sinsemellan? Har man i organisationen till exempel fattat ett beslut om användning av egna terminaler, såsom mobiltelefoner, för att sköta arbetsärenden? Detta kan skapa effektivitet och flexibilitet i arbetet, men samtidigt innebär det att organisationen inte lika bra kan se de cyberhot som riktas mot organisationen.

DEL VI

Säkerhetskultur

Organisationer fokuserar ofta på tekniska frågor kring cybersäkerhet och åsidosätter människors behov och deras dagliga arbetssätt. Detta är sällan ett framgångsrecept. Om den officiella praxisen försvårar arbetet eller gör det långsammare, försöker människor hitta genvägar och inofficiella sätt att utföra sina uppgifter. Det är därmed bra att förstå att personalen inte engagerar sig i cybersäkerheten utan en god säkerhetskultur.

I vissa organisationer anses personalen vara cybersäkerhetens "svaga länk". Vi måste göra oss av med detta tänkesätt.

Vad kan styrelsen göra?

Föregå med gott exempel

Styrelsen och högsta ledningen har en stor inverkan på andras attityder. Det är möjligt att högsta ledningen inte behöver iaktta säkerhetspraxis och -processer eller får annan slags särbehandling, som till exempel utrustning som frångår organisationens IT-policy. Detta sänder ett meddelande till den övriga organisationen om att reglerna inte nödvändigtvis anses ändamålsenliga eller att man får kringgå dem.

Om ledningen och styrelsemedlemmarna inte själva följer den praxis man kommit överens om i organisationen, kommer knappast någon annan att göra det heller. Om en viss praxis har en skadlig inverkan på organisationen, ska den göras om till det bättre.

Det tar tid att utveckla en kultur och det kräver gemensamma satsningar. Den säkerhetsattityd som styrelsen och ledningen kräver sprids inte automatiskt till hela organisationen.

Vad kan man göra inom organisationen?

Sätt personalen i centrum för säkerheten

I vissa organisationer anses personalen vara cybersäkerhetens svaga länk. Vi måste göra oss av med detta tankesätt. För att realisera cybersäkerheten effektivt krävs det balans mellan alla olika faktorer – inte enbart ett antagande om att människor alltid böjer sig för teknologins krav. Om personalen försöker kringgå avtalade handlingsmodeller, kan det indikera att praxis eller processer behöver revideras.

En utbildad och uppmärksam personal har en central roll när det gäller att upptäcka säkerhetsincidenter. Inom organisationen ska man säkerställa att personalen rapporterar om hot och incidenter som de lägger märke till och att det finns tydliga processer för hur dessa ska hanteras.

Mot en kultur av öppenhet

Säkerställ att personalen uppmuntras att prata och rapportera om sina bekymmer. Samtidigt ska man sträva efter att ändamålsenliga åtgärder vidtas utifrån dessa, inte att hitta skyldiga. På detta sätt kan personalen fokusera på att utveckla organisationens säkerhet istället för på att skydda sig själva.

Att fundera på

Hur kan styrelsemedlemmarna och ledningen föregå med gott exempel?

- Säkerställ att arbetstagarna upplever att de kan påverka organisationens säkerhet och att de har redskap för att föra fram sina säkerhetsbekymmer.
- Förbind er till de beslut om säkerhet som redan fattats, tillämpa dem och lyft fram ineffektiv praxis i samarbete med arbetstagarna.
- Säkerställ att ni i organisationen talar öppet och positivt till personalen om var för cybersäkerhet är viktigt.

Råder det en god säkerhetskultur i vår organisation?
Tecken på en god säkerhetskultur är till exempel att:

- Personalen vet hur och till vem de kan rapportera om bekymmer eller incidenter. De upplever också att de uppmuntras att rapportera.
- Personalen är inte rädd för negativa följder av sina rapporter om bekymmer eller incidenter.
- Personalen upplever att de kan ifrågasätta handlingsmodeller på ett konstruktivt sätt.
- Personalens synpunkter utnyttjas genuint i utformningen av säkerhetspraxis.
- Personalen förstår vikten av cybersäkerhet och dess betydelse för organisatio nen.
- Istället för misslyckanden fokuserar man i rapporteringen och den interna kom munikationen på framgångar (man berättar till exempel hur många som rappor terat om nätfiskemeddelanden, inte om hur många som gick på dem).

DEL VII

Cybersäkerhetskompetens

Efterfrågan på cybersäkerhetsexperter ökar hela tiden. Det här skapar utmaningar för tillgången till den kompetens som organisationerna behöver. Det är därför viktigt att organisationen funderar på vilken slags expertis som behövs nu och i framtiden och hur organisationen ska skaffa den kompetens som behövs.

Vad kan styrelsen göra?

Skapa en förståelse för situationen vid er organisation

Finns det en informationssäkerhetschef eller -ledare vid organisationen? Hur är det med en informationssäkerhetsgrupp? Finns det någon som har ansvaret för incidenthantering? Om det inte finns, borde det finnas?

Svaren på de här frågorna ger en bild av cybersäkerhetsförmågan vid organisationen och skapar en förståelse för varifrån de uppgifter om cybersäkerhet som styrelsen fått kommer.

Det lönar sig också för styrelsen att fundera på sin egen sakkunskap. Finns det för tillfället tillräcklig sakkunskap i styrelsen för att säkerställa att styrelsen har förmågan att fatta de strategiska beslut om cybersäkerhet som behövs? Hänger styrelsen med i utvecklingen, då nya teknologier innebär nya säkerhetsutmaningar?

Enligt en studie som Global Information Security Workforce gjort kommer det att fram till 2022 uppstå en brist som motsvarar 350 000 cybersäkerhetsexperter.

Vad kan man göra inom organisationen?

Gör upp en plan

Organisationen ska reda ut vilken typ av sakkunskap inom cybersäkerhet den behöver. Inom cybersäkerhet behövs många olika typer av kompetens, som kan vara allt från till exempel informationsnätens säkerhet till risk- och incidenthantering. Det lönar sig att först fundera närmare på vilken kompetens organisationen behöver för att uppnå de viktigaste målen och för att kunna hantera risker och att som följande steg avgöra till vilka delar denna kompetens inte kan skaffas externt.

Fatta beslut om hur snabbt organisationen behöver kompetensen. Om tanken är att utveckla den nuvarande personalens kompetens, är det viktigt att komma ihåg att det behövs tid för att uppnå tillräcklig sakkunskap. En enskild kurs gör inte någon till en expert inom cybersäkerhet – man måste också få möjlighet att utveckla sitt praktiska kunnande. Om organisationen behöver sakkunskap snabbt, är det ofta ett bättre alternativ att anlita en konsult eller en expert.

Att fundera på

Hurdan sakkunskap inom cybersäkerhet behöver er organisation och hurdan kompetens har er organisation redan?

- Vilken sakkunskap behöver er organisation för att kunna hantera cyberrisker?
- Vilka arbetsuppgifter ska behållas internt och vilka lönar det sig att lägga ut?
- Vilken kunskap ska varje anställd vid organisationen ha om cybersäkerhet?
- Hur ofta och hur bra organiserarar vi utbildning om säkerhetspraxis för de anställda? Hur är det med särskilda hot som vår organisation är sårbar för?

Hurdan plan har organisationen för att utveckla den kompetens som saknas?

- Vem ansvarar för att utveckla sakkunskapen om cybersäkerhet?
- Har man en plan för utvecklingen och inför vem svarar de ansvariga för att den genomförs?
- Var hittas de personer som behövs? Arbetar de för vår organisation eller skaffas den kompetens som krävs till exempel externt?
- Hur kan styrelsen stöda arbetet?

Har styrelsen tillräckligt med kunnande och sakkunskap så att den kan vara ansvarig för alla beslut om cybersäkerhet?

- Är man i styrelsen tillräckligt insatt i de beslut om cybersäkerhet som ska fattas inom organisationen?
- Om så inte är fallet, hur kan styrelsemedlemmarna bli mera insatta?
    - Ni kan börja genom att läsa inledningen till den del i denna guide som handlar om cybersäkerhet. På många håll ordnas också utbildning i cybersäkerhet som särskilt är avsedd för styrelsemedlemmar.

Hur ser vi till att vi har en personal som kan svara på framtida utmaningar inom cybersäkerhet?

- Får vi den information som behövs om organisationens kompetens- och rekryteringsbehov inom cybersäkerhet?
- Använder vi olika rekryteringskanaler mångsidigt?

DEL VIII

Uppföljning av åtgärdernas effekt

Redan genom att genomföra mycket enkla åtgärder kan man minska sannolikheten för eller följderna av incidenter.

Vad kan styrelsen göra?

Fördjupa er en aning i teknologi

PEn grundförståelse för cybersäkerhet gör det enklare för styrelsemedlemmarna att ställa de rätta frågorna för att de ska kunna säkerställa nivån på organisationens cybersäkerhet. Ni kan börja med att diskutera de nuvarande cybersäkerhetsåtgärderna med organisationens experter. Följande frågor ger en bild av vad det lönar sig att diskutera.

Vad kan man göra inom organisationen?

Börja från cybersäkerhetens grundnivå

Angriparna använder sig ofta av vanliga, offentligt tillgängliga applikationer och metoder. Detta kan till stor del avvärjas genom att se till att man har en grundläggande cybersäkerhet. Det finns flera olika ramverk som specificerar åtgärderna för en god grundläggande nivå av cybersäkerhet. Bland dessa kan nämnas ISO/IEC 27000-säkerhetsstandarderna och NIST:s (National Institute of Standards and Technology) cybersäkerhetsramverk. År 2020 kommer Cybersäkerhetscentret att publicera ett nationellt utvärderingsinstrument. Med instrumentet kan organisationen bedöma statusen för den egna cybersäkerheten.

Skräddarsy åtgärderna enligt era största hotfaktorer

Åtgärderna inom den grundläggande cybersäkerheten hjälper er att avvärja de vanligaste cyberangreppen. När den grundläggande nivån fastställts och uppnåtts är det skäl att genomföra åtgärder för att hantera prioriterade risker. De här åtgärderna skräddarsys enligt affärsverksamhetsmålen, organisationens tekniska miljö och organisationens hotprofil (att skydda sig mot specifika hot och/eller angripare).

Med hjälp av en informationssäkerhetsarkitektur som har många olika lager är man beredd på att om ett enskilt delområde ger vika eller en angripare lyckas bryta sig igenom ett lager, så hindrar följande lager angriparen från att komma vidare. Vid organisationen borde man samtidigt genomföra flera olika åtgärder, som när de används tillsammans bidrar till att minska följderna av cyberhot. När organisationen har fastställt sina mål för cybersäkerheten kan man koncentrera sig på att bygga upp de olika skyddslagren kring de viktigaste elementen.

Cybersäkerhetscentrets HAVARO-system observerar och informerar organisationer om allvarliga kränkningar av informationssäkerheten. Sådana är till exempel informationssäkerhetshot som har följder för organisationens ekonomi, organisationens information eller affärsverksamhetens kontinuitet. Läs mera om HAVARO-tjänsten på https://www.kyberturvallisuuskeskus.fi/sv/havaro-tjansten

Skydda er också mot interna hot

Skyddsåtgärderna upphör inte vid gränsen till organisationens nätverk. När man har ett gott skydd utgår man från att en angripare när som helst kan ta sig in i organisationens nätverk. Vid skyddet av det interna kommunikationsnätet strävar man efter att minimera de skador som en angripare kan orsaka.

Här är identitets- och åtkomsthantering en av de viktigaste åtgärderna. Vanliga metoder är en effektiv hantering av användarnas behörigheter och att dela in organisationens nätverk i delar, det vill säga segmentering. Att så snabbt som möjligt identifiera intrång i systemet minskar angriparens möjligheter att vålla skador. Att samla in logguppgifter och följa upp dem är centrala åtgärder för att upptäcka skadlig verksamhet av detta slag.

De här åtgärderna bidrar också till att begränsa det hot som kommer internt från organisationen. Med detta avses en person som har tillstånd att använda systemen, men som strävar efter att skada organisationen. Det här hotet kan vara allt från en anställd som utför otillåtna åtgärder till organiserat företagsspionage.

Kontrollera och utvärdera åtgärderna

God cybersäkerhet handlar om en kontinuerlig verksamhet som består av tillgång till den rätta och tillräcklig information, beslut som är baserade på informationen och åtgärder för att minska riskerna. Organisationen ska utvärdera och anpassa sina skyddsåtgärder enligt hur organisationen och organisationens hotprofil ändras. Därför är det viktigt att man har verktyg för att utvärdera hur effektiva organisationens åtgärder är.

Man kan utvärdera hur effektiva åtgärderna är på olika sätt. Man kan till exempel testa hur säkra organisationens nätverk och tjänster är (så kallat penetrationstest) eller genom att simulera processens funktionalitet. Man kan också kombinera interna utvärderingsåtgärder med en utvärdering som genomförs av en extern aktör.

Genom att göra de anställda delaktiga kan man få en mera noggrann bild av hur effektiva de åtgärder som organisationen genomfört är. På det här sättet kan man också få värdefull information om hur man kan förbättra tillvägagångssätt och processer. Olika mätare och indikatorer kan visa inom vilka områden organisationen borde ändra eller utveckla sin verksamhet.

Att fundera på

Hur kan vår organisation försäkra sig om att våra åtgärder är effektiva?

För att säkerställa detta kan organisationen vidta till exempel följande åtgärder:

- Penetrationstest genomfört av en extern organisation och utvecklingsåtgärder som genomförts utifrån det.
- Automatisk testning av skyddsåtgärder och loggföring och uppföljning av verksamheten i nätet.
- Utvärdering av vidtagna åtgärder utifrån lämpliga ramverk. Utvärderingen kan endera genomföras internt eller av en oberoende konsult. Lämpliga ramverk är tillexempel ISO/IEC 27002 standarden, NIST:s cybersäkerhetsramverk eller Cyber-säkerhetscentrets nationella utvärderingsinstrument.
- Man ser till att hotbedömningen och tyngdpunkterna inom cybersäkerhet granskas regelbundet och att skyddsåtgärderna uppdateras enligt detta.
- Man ser till att tyngdpunkterna för cybersäkerhetsåtgärderna är de samma som de risker styrelsen identifierat och betonat.

Vilka åtgärder har vår organisation vidtagit för att minimera de skador ett angrepp kan orsaka?

Se till att ni inom organisationen funderar till exempel på:

- Hur verifieras användare och datorterminaler och hur beviljas användar-rättigheter?
- Hur kan man upptäcka att det finns en angripare i organisationens nätverk?
- Hålls organisationens nätverk åtskilda så att en angripare inte via en apparat eller en domän kan ta sig till andra domäner inom organisationen?

På vilket sätt är vår organisation skyddad mot nätfiskeangrepp?

- Vi filtrerar eller blockerar inkommande nätfiskemeddelanden i e-posten.
- Vi ser till att extern e-post markerats som extern e-post.
- Vi hindrar angripare från att förfalska våra egna e-postmeddelanden.
- Vi hjälper våra anställda att känna igen misstänkta e-postmeddelanden och att rapportera om dem.

Hur övervakar vår organisation användningen av behörigheterna till informtionstekniska användarkonton?

- När vi skapar personalens användarkonton tillämpar vi principen om minsta möjliga behörighet.
- Vi begränsar följderna av ett angrepp genom att övervaka användarkonton med behörigheter.

På vilket sätt ser vår organisation till att vår programvara och våra apparater är uppdaterade?

- Vi har fastställt processer som vi använder för att upptäcka, klassificera och åtgärda sårbarheter som kan utnyttjas i vår tekniska miljö.
- Vi har gjort upp planer för slutskedet av livscykeln för apparater och program som inte längre stöds.
- Vår nätverksarkitektur minimerar de skador som en angripare kan orsaka.
- Vi utnyttjar på lämpligt sätt tjänster eller molntjänster från en tredje part och fokuserar på de områden vi kan påverka mest.

Hur har identifieringen av personer och tillgången till systemen ordnats?

- Vid organisationen används god praxis för lösenord.
- Vid organisationen används tvåfaktorsautentisering alltid då det är möjligt.

DEL IX

Samarbete

Cybersäkerhet är centralt när man samarbetar med tjänsteleverantörer och kompanjoner. Det här beror på att:

- Olika rutter att utifrån ta sig in i organisatio nen ökar då antalet anslutningar och tjänster ökar. Om någon av dem utsätts för fara innebär det en risk mot hela organisationen.
- Man via er organisation kan försöka göra intrång i en annan organisation som ni erbjuder tjänster.
- Man kan försöka göra intrång i er organisation via era tjänsteleverantörer.
- Er organisation kan behandla uppgifter som är känsliga eller värdefulla för er kompanjon.

Vad kan styrelsen göra?

Inkludera cybersäkerhet i besluten

Alla organisationer samarbetar med minst en annan organisation. Samarbete mellan organisationer innebär tillgång till organisationernas IT-system, nätverk eller information. Försäkra er om följande tre saker:

1. Se till att en angripare inte erbjudes en rutt att ta sig in i er organisation.
2. Alla era kompanjoner och tjänsteleverantörer behandlar er organisations känsliga uppgifter tillbörligt och säkert.
3. Cybersäkerhet har beaktats i alla köpta pro dukter eller tjänster.

Cybersäkerhet ska ingå i alla beslut som gäller nya samarbeten eller kompanjonskap. Det här omfattar beslut som gäller tjänsteleverantörer, varuleverantörer, fusioner, företagsköp och kompanjoner. Det lönar sig också att se till att ansvarsfördelningen och skyldigheterna i etablerade samarbeten är uppdaterade.

Vad kan man göra inom organisationen?

Fastställ de säkerhetskrav som ni förväntar er att era tjänsteleverantörer och kompanjoner uppfyller och ge dem tydlig information om era förväntningar.

Se över arrangemangen med era nuvarande tjänsteleverantörer och se till att säkerhetskraven för dem har beaktats. Om er organisation själv är en tjänsteleverantör ska ni också fylla de säkerhetskrav som kunden ställer.

Se till att de säkerhetskrav som ni fastställt är motiverade, har rätt dimension och är lämpliga för de bedömda riskerna. Ta tjänsteleverantörernas nuvarande situation i beaktande och ge dem tillräckligt med tid för att göra de förbättringar som behövs.

Be om garantier

Säkerhet ska redan från början inkluderas i alla avtal. Organisationen måste kunna lita på att de säkerhetskrav man kommit överens om uppfylls. Det här kan säkerställas till exempel med tester, kontroller eller genom hur standarder uppfylls. Det lönar sig att tillsammans med kompanjonerna öva på processerna i samband med incidenthantering och på att upprätthålla cybersäkerhet.

Kom ihåg följderna av ett eventuellt hot mot en tjänsteleverantör.

Oberoende av vilka avtal ni ingått med era kompanjoner eller hurdan cybersäkerhet era kompanjoner har, måste ni utgå från att de i något skede kommer att utsättas för fara. Planera era nätverk, IT-system och informationens säkerhet utifrån detta antagande. Ta också denna eventualitet i beaktande i avtal om säkerhet. Hur förväntar ni er att era kompanjoner ska agera? Ska de till exempel informera er organisation om incidenter?

Att fundera på

På vilket sätt begränsar er organisation de risker som uppstår när man delar information, IT-system och anslutningar med andra organisationer?

Se till att:

- Organisationen är väl insatt i sina tjänsteleverantörer och i vilka IT-system och vilken information de har tillgång till. Det behövs också en process för att bevilja och avsluta åtkomsträttigheter.
- Definiera klart och tydligt era förväntningar på hur kompanjonerna ska skydda er organisations information och använda era IT-system.
- Inkludera redan i inledningsskedet cybersäkerhet i alla era avtal.

Gör så här:

- Om ett stort antal företag ingår i leveranskedjan ska ni tillsammans med de viktigaste tjänsteleverantörerna komma överens om deras anmälningsskyldig heter till er och de processer som styr deras underleverantörer.
- Välj sådana organisationer som kan visa att deras verksamhet är säker.
- Minimera andra organisationers åtkomst till era tjänster och ert informations-utbyte med dem.
- Verifiera och bekräfta underleverantörernas användare innan användar-rättigheterna beviljas.

På vilket sätt ser vår organisation till att cybersäkerhet beaktas i beslut som gäller affärsverksamheten?

- Se till att cybersäkerhet är en del av organisationens kultur och strategi.
- Se till att cybersäkerhet är en medveten del av alla beslut om förvärv, fusioner eller företagsköp.

Är vår organisation säker på att vi som tjänsteleverantör uppfyller alla säkerhetskrav?

- Om organisationen erbjuder andra organisationer tjänster, innebär detta att den har större risker. Se till att organisationen är beredd att agera i situationer där de kunduppgifter som ni besitter äventyras.

Har er organisation klara och tydliga villkor om användning av tjänsteleverantörer? Har vi informerat om dem? Har följande frågor klart och tydligt beskrivits i strategierna och anvisningarna om tjänsteleverantörer och anskaffningar?

- Vilka risker är organisationen beredd att acceptera när den anlitar tjänste-leverantörer? Till exempel kan den risk för ett dåligt rykte som uppstår i onormala situationer vara mindre om tjänsteleverantören är ansvarig. Den ekonomiska risken kan dock vara lika stor som utan tjänsteleverantör.
- Vilka förväntningar har organisationen på tjänsteleverantörernas säkerhet? Hur mycket är leverantören beredd att betala för en bättre säkerhetsnivå?

DEL X

När det värsta händer

En kränkning av informationssäkerheten kan ha stora följder för organisationens ekonomi, produktivitet och rykte. Incidenten kan också utvecklas till en cyberstörning som i stor utsträckning påverkar hela organisationens verksamhet. Om man har förberett sig på att upptäcka och snabbt reagera på kränkningar har man större möjligheter att begränsa skadorna. Detta leder också till mindre ekonomisk skada och andra följder för verksamheten.

Cybersäkerhetsverket hjälper alla finländska organisationer som utsatts för kränkningar av informationssäkerheten. Cybersäkerhetscentrets kontaktuppgifter finns på guidens baksida.

Vad kan styrelsen göra?

Se till att organisationen har en plan

En stor del av de finländska organisationerna har ingen plan för hur man ska agera vid kränkningar av informationssäkerheten eller i allvarliga störningssituationer som de leder till. Se till att organisationen har en plan för kränkningar av informationssäkerheten och allvarliga störningssituationer.

Förstå er roll i hanteringen av kränkningar av informationssäkerheten

I synnerhet vid omfattande störningar försämras individernas och organisationernas förmåga att fatta beslut. Därför ska alla redan innan något händer sätta sig in i sin roll och i hur man ska gå tillväga vid organisationen.

Styrelsen ska tydligt informera om när den ska rapporteras om kränkningar av informationssäkerheten.

- I vilket skede ska styrelsen informeras om en kränkning?
- Hurdana kränkningar överskrider tröskeln för att göra en anmälan?

Delta i övningarna

Det bästa sättet att testa organisationens processer och roller är att öva hanteringen av cyberstörningssituationer. Om det i en persons uppgifter ingår att delta i hanteringen av en verklig störning, ska detta också övas. När man övar tillsammans med personalen kan man samtidigt upptäcka problem till exempel inom beslutsfattandet. Man kan tänka sig övningen som en kris i organisationen, där man själv kan välja tidpunkt och konsekvenser. Man kan få många värdefulla lärdomar av en krissituation och med hjälp av en övning kan man tillämpa denna inlärningsform utan att krisen stör organisationens verksamhet.

Främja en kultur där man inte letar efter skyldiga

I analyserna efter en kränkning av informationssäkerheten strävar man efter att minska sannolikheten för nya kränkningar och deras följder i framtiden. Det viktigaste är att man ser ärligt och objektivt på det som hänt. I en organisation där man inte hela tiden strävar efter att hitta den skyldiga lyckas man med detta. Det lönar sig för styrelsen att beakta att den största delen av bestämmelserna, till exempel EU:s allmänna dataskyddsförordning, överför ansvaret för en kränkning av informationssäkerheten på hela organisationen och inte på enskilda personer. Styrelsen är därför som förvaltningsorgan i sista hand ansvarig för alla incidenter i organisationens cybersäkerhet.

Vad kan man göra inom organisationen?

Ta reda på hur en kränkning av informationssäkerheten kan se ut

En av de främsta aspekterna som inte beaktas är att definiera vad som avses med en kränkning av informationssäkerheten. Detta har två synvinklar:

- hur kan man överhuvudtaget upptäcka en händelse eller en incident?
- i vilket skede blir händelsen eller incidenten en kränkning av informations säkerheten?
- i vilket skede blir det en så allvarlig störning att situationen kräver handlings modeller som avviker från de normala processerna?

HUR KAN MAN UPPTÄCKA VAD SOM HÄNT?

Med uppföljning avses granskning av information från nätverk eller IT-system eller från loggar för att upptäcka sådana incidenter som kan tyda på skadlig verksamhet. Även om man inte använder sig av egentliga uppföljningsmekanismer, är det viktigt att samla in information från IT-systemens och nätverkens loggar. Informationen kan användas för att reda ut incidenter och i fortsättningen också för att skydda sig från dem.

NÄR BLIR HÄNDELSEN EN KRÄNKNING AV INFORMATIONSSÄKERHETEN?

Det här är inte alltid en entydig fråga. Organisationen kan försöka samla in så mycket information som möjligt för att kunna göra en bedömning av ”händelsen”, men den har troligen ändå inte en helhetsbild av vad som hänt. Att reda ut händelsen och reagera på den kan orsaka kostnader. Om händelsen är allvarlig kan den påverka organisationens rykte och produktivitet. Organisationen borde också på förhand bestämma vem som har befogenheter att fatta beslut om att man ska reagera på händelsen och vilka tröskelvärdena är för beslutsfattandet.

Man ska också planera hur man begränsar följderna för kompanjoner eller kunder om organisationens cybersäkerhet hotats. När ska de informeras? Hur kan man begränsa de skador som de orsakas?

Man ska också fundera på hur organisationen agerar om en tjänsteleverantörs informationssäkerhet hotas. Organisationen kan inte nödvändigtvis påverka hur en tjänsteleverantör hanterar en kränkning av informationssäkerheten. Vad kan organisationen på egen hand göra för att begränsa följderna?

VAD ÄR EN KRÄNKNING AV INFORMATIONSSÄKERHETEN?

Med en kränkning av informationssäkerheten avses kränkning av ett IT-systems eller en tjänsts säkerhet. I allmänhet handlar det om något av följande:

- intrång eller försök till intrång i IT-systemet och/eller i informationen
- otillåten användning av IT-system som används för behandling eller lagring av information
- ändringar i IT-systemens inbyggda program, program eller apparater utan ägarens tillstånd
- avsiktlig störning eller blockering av tjänst.

Utnyttja den information som redan finns

Information som samlats in från hot och tekniska miljöer är till stor nytta på två sätt:

- Den ger information om incidentens följder. Vad kan angriparen ha tillgång till om hen tagit sig in i en viss apparat? Kan angriparen få tag på kritiska element i er organisation?
- Den är till hjälp när man fastställer de åtgärder som ska vidtas. Är det möjligt att isolera ett särskilt nätverk, om angriparen tagit sig in i det? Om det är möjligt att isolera nätverket, vilka följder har det för organisationens verksamhet?

Vidta förebyggande åtgärder

Vidta åtgärder som begränsar den skada ett angrepp kan orsaka. Sådana åtgärder kan vara:

- att begränsa hur angripare som tagit sig in organisationens nätverk kan ta sig vidare
- att förebyggande begränsa följderna av ett angrepp – till exempel genom att säkerhetskopiera material kan man begränsa följderna av ett utpressningsvirus.

Som med andra skyddsåtgärder ska de här skyddsåtgärderna fokusera på att skydda de element som är viktigast för organisationen.

Gör upp en plan för hantering av kränkningar av informationssäkerheten och de cyberstörningar som de orsakar

Förutom de tekniska delområdena ska planen omfatta:

- människor och processer, som medier samt informering av kunder och intressentgrupper
- anmälan till Cybersäkerhetscentret
- rapportering till regleringsmyndigheterna
- brottsanmälan till polisen.

För de vanligaste incidenterna kan det löna sig att göra upp en särskild plan där man bestämmer organisationens åtgärder. Kom också ihåg att öva!

Erfarenheter

Efter en kränkning av informationssäkerheten glömmer man ofta bort att utvärdera händelsen. En kränkning kan ge viktig information om organisationens cybersäkerhet. Till exempel:

1. Hot som riktats mot organisationen
   - Vem angrep? Var angreppet riktat?
   - Genomfördes angreppet så som man förväntat sig?
   - Var målen för angreppet de som man förväntat sig?

2. Hur effektiva var skyddsåtgärderna?
   - Vad skyddade skyddsåtgärderna?
   - Vad skyddade de inte?
   - Kan de förbättras?

3. Hur effektiva var de åtgärder som vidtogs när man reagerade på kränkningen?
   - Vad borde man ha gjort annorlunda?
   - Hjälpte åtgärderna till med att begränsa följderna av kränkningen?
   - Gjorde de något värre eller svårare?

Cybersäkerhetscentret hjälper organisationer att ordna övningar. Med hjälp av våra tjänster kan organisationer starta sina egna övningar eller få experthjälp med planering av innehållet i ett existerande övningsprogram. Mera information om övningsverksamheten på https://www.kyberturvallisuuskeskus.fi/sv/vara-tjanster/ovningar

Att fundera på

Finns det en plan för hantering av IT-incidenter? Hur ser ni till att planen är effektiv? Planen ska åtminstone innehålla följande:

- Viktiga interna och externa kontaktuppgifter.
- Tydliga eskaleringsrutiner (till exempel för den högsta ledningen) och bestämda processer för att fatta kritiska beslut.
- Tydlig ansvarsfördelning och ett omnämnande om den gäller ordinarie arbetstid eller om den alltid gäller.
- En allmän flödesplan eller processbeskrivning för händelsens och informationssäkerhetskränkningens hela livscykel.
- Anvisningar om krav i lagstiftningen, till exempel när en kränkning av informations säkerheten ska anmälas och åt vem.

Vet vi i vår organisation varifrån vi kan be om hjälp i samband med en kränkning av informationssäkerheten?

- Har vi en förteckning över viktiga kontaktuppgifter?
- Har rätt personer tillgång till kontaktuppgifterna också i en situation där man inte kan använda IT-system?

Tar vi som organisation lärdom av kränkningar av informationssäkerheten och nära ögat-situationer?

- Sammanställer organisationen det vi lärt oss och de erfarenheter vi fått?
- Utvecklas organisationens verksamhet utifrån dem?

Hur får vår organisation vetskap om kränkningar av informationssäkerheten?

- Hur övervakar man inom organisationen kritisk information (till exempel personuppgifter), som det är av betydelse om den utsätts för fara, förloras eller ändras?
- Vem granskar logguppgifterna? Har den här personen tillräcklig utbildning för att känna igen avvikande verksamhet?
- Hur kan personalen rapportera om misstänkt verksamhet?
- Har larmtrösklarna rätt nivå? Är de tillräckligt låga för att en lämplig varning om eventuella incidenter ska kunna ges? Eller tillräckligt höga så att de personer som behandlar dem inte belastas med information som inte är av betydelse?

När man ser närmare på den interna kunskapsdelningen vid kränkningar av informationssäkerheten ska organisationen beakta:

- Vad är en kränkning av informationssäkerheten?
- Vem har befogenheter att avgöra om det handlar om en kränkning av informationssäkerheten?
- Vem ska ha mera detaljerad information om kränkningen av informationssäkerheten?
- Har styrelsen gett klara och tydliga anvisningar om tröskeln för att den ska meddelas?

Vet styrelsen vem som leder verksamheten vid kränkningar av informationssäkerheten och vem som har befogenheter att fatta beslut?

Det här är beroende av organisationens struktur. Styrelsemedlemmarna, den verkställande direktören eller någon av cheferna kan ha befogenheterna, eller så kan de vara delade mellan olika uppgifter. Se inom organisationen i mån av möjlighet bland annat på:

- Vem kan fatta beslut i vilka frågor? Undvik att personifiera ansvaret om det är möjligt. Ansvaret ska i stället ges åt en uppgift eller funktion.
- Gör upp reservplaner ifall de aktuella beslutsfattarna inte går att nås.
- Öva inom organisationen på hur förfarandet för beslutsfattande fungerar.

Bilaga I

Viktig lagstiftning

Lag om tjänster inom elektronisk kommunikation (917/2014)

Den viktigaste lagen om elektronisk kommunikation i Finland är lagen om tjänster inom elektronisk kommunikation (917/2014). I lagen finns omfattande bestämmelser bland annat om informationssäkerhet och att trygga konfidentiell kommunikation. Bestämmelserna gäller teleföretag, kommunikationsförmedlare, sammanslutningsabonnenter och registrarer. För den största delen av de finländska organisationerna är bestämmelserna om sammanslutningsabonnenter de viktigaste. Med sammanslutningsabonnent avses ett företag eller en organisation som abonnerar på kommunikationstjänster eller mervärdestjänster och som i sitt kommunikationsnät behandlar meddelanden från användare samt förmedlingsuppgifter och lokaliseringsuppgifter. En sammanslutningsabonnent kan alltså vara en näringsidkare, ett andelslag, ett aktiebolag, en förening, en läroanstalt eller statens ämbetsverk. Sammanslutningsabonnenten kan till exempel vara ett företag som skaffar och erbjuder telefon- eller bredbandsabonnemang åt sina anställda och WLAN-abonnemang åt dem som besöker verksamhetslokalerna. Om sammanslutningsabonnenters funktion, informationssäkerhet och tryggande av konfidentiell kommunikation bestäms i synnerhet i avdelning VI och X i lagen.

EU:s direktiv om nät- och informationssäkerhet (s.k. NIS-direktivet)

Med EU:s direktiv om nät- och informationssäkerhet strävar man efter en högklassig säkerhet i nätverks- och IT-system i hela unionen. I direktivet regleras informationssäkerhetsskyldigheter och rapportering vid störningar.

Med bestämmelserna förpliktigar man de centrala tjänsteleverantörerna och vissa aktörer som erbjuder digitala tjänster att ha en omfattande hantering av informationssäkerhetsrisker, hantering av tjänsternas kontinuitet vid incidenter samt att rapportera de ansvariga myndigheterna om incidenter som stör eller hotar verksamhetens kontinuitet.

Skyldigheterna i direktivet gäller branscher som är viktiga med tanke på att samhället ska fungera. I Finland har direktivet satts i kraft i den sektorsvisa lagstiftningen. De branschvisa myndigheterna övervakar att lagarna efterlevs.

- Trafik och transport - Traficom
- Energiförsörjningen - Energimyndigheten
- Social- och hälsovård - Valvira
- Finansbranschen - Finansinspektionen
- Finansbranschens infrastruktur - Finansinspektionen
- Vattentjänster - NTM-centralerna
- Digital infrastruktur - Traficom
- Digitala tjänster - Traficom

EU:s allmänna dataskyddsförordning

I den allmänna dataskyddsförordningen fastställs detaljerade skyldigheter för företag och organisationer som samlar in, lagrar och behandlar personuppgifter. Reglerna gäller både europeiska organisationer som behandlar personuppgifter i EU och organisationer baserade utanför EU som behandlar personuppgifter för personer som bor inom EU. Den allmänna dataskyddsförordningen tillämpas om företaget behandlar personuppgifter och är baserat i EU. Den tillämpas oavsett var den egentliga behandlingen sker eller om ditt företag är baserat utanför EU men behandlar personuppgifter för att erbjuda varor eller tjänster i EU eller övervaka fysiska personers beteende i EU.

Dataskyddslag (1050/2018)

Dataskyddslagen preciserar och kompletterar EU:s allmänna dataskyddsförordning. Lagen är en allmän lag som ska tillämpas på behandling av personuppgifter. I och med att den kompletterar och preciserar den allmänna dataskyddsförordningen utgör den ingen självständig och samlad lagstiftningshelhet, utan den ska tillämpas parallellt med den allmänna dataskyddsförordningen.

Strafflagen (39/1889)

Finlands strafflag är inte bekant med begreppet cyberbrott. Cyberbrott definieras i regel som informations- och kommunikationsbrott. Särskilda bestämmelser om dessa finns i 38 kap. i strafflagen. Det finns också i andra kapitel i strafflagen bestämmelser om brott som ansluter till cyberbrott. I kap. 30 i strafflagen, som handlar om näringsbrott, finns till exempel skilda bestämmelser om brott mot företagshemlighet och missbruk av företagshemlighet.

Bilaga II

Myndighetsorganisationer i Finland

Cybersäkerhetscentret vid Transport- och kommunikationsverket

Cybersäkerhetscentret vid Transport- och kommunikationsverket Traficom är en nationell informationssäkerhetsmyndighet som har följande uppgifter:

- samla in information om informationssäkerhetskränkningar och om hot om sådana
- informera om informationssäkerhetsfrågor och om hur kommunikationsnät och -tjänster fungerar;
- reda ut kränkningar och hot om kränkningar av informationssäkerheten för nättjänster, kommunikationstjänster och mervärdestjänster
- övervaka och styra teleföretags informationssäkerhet och beredskap
- inspektera och godkänna system och nätverk
- övervaka skyldigheter i samband med integritetsskydd vid elektronisk kommunikation

Privatpersoner, företag och organisationer kan konfidentiellt anmäla kränkningar av informationssäkerheten de blivit utsatta för, t.ex. misstänkta skadliga program, nätfiske eller överbelastningsangrepp, samt kränkningsförsök till Cybersäkerhetscentret. På basis av anmälningarna kan Cybersäkerhetscentret vid behov erbjuda hjälp med att utreda och undersöka informationssäkerhetskränkningar samt koordinera nödvändiga åtgärder.

Du kan göra en anmälan om kränkning av informationssäkerheten till Cybersäkerhetscentrets e-post cert@traficom.fi och på webbplatsen https://www.kyberturvallisuuskeskus.fi/sv via knappen "anmäl kränkningar".

Mera om Cybersäkerhetscentret på https://www.kyberturvallisuuskeskus.fi/sv/

Polisen

När det gäller att förebygga, utreda och åtalspröva IT-brott är det i regel polisen som är behörig myndighet i samarbete med andra brottsbekämpande myndigheter. Också Tullen och Gränsbevakningsväsendet utreder brott inom sina områden, vilket även inbegriper brott som begås med hjälp av informationsnät och informationsteknik. Majoriteten av IT-brotten utreds av den lokala polisen. Alla polisinrättningar har enheter som är specialiserade på behandling och analysering av digitalt bevismaterial. Polisens riksomfattande rådgivningstjänst finns på telefonnummer 0295 419 800 (vardagar 08–16.15) / neuvontapalvelu@poliisi.fi

Centralkriminalpolisen (CKP) är en riksomfattande polisenhet vars verksamhetsområde är hela Finland. Vid Centralkriminalpolisen finns en enhet med inriktning på förundersökning av IT-brott, Centralen för bekämpning av cyberbrott, där man fokuserar på att utreda större internationella brottshelheter som huvudsakligen sker i IT-miljö. Du kan i ett brottmål lämna in en begäran om utredning till CKP, men utredningen kan enligt prövningsrätten överföras åt den lokala polisinrättningen. CKP:s växel har telefonnumret 0295 480 141 (må-fre 08–16.15).

Du kan också göra en brottsanmälan eller anmälan om en cyberincident via webben på https://www.poliisi.fi/brott/elektronisk_brottsanmalan eller https://www.poliisi.fi/nattips. Nättips är ett forum där man kan anmäla också de minsta cyberstörningarna, som inte uppfyller brottsrekvisitet.

Skyddspolisen

Skyddspolisen är en säkerhets- och underrättelsetjänst, som underrättar om och förebygger hot mot statens säkerhet. Därtill tillhandahåller Skyddspolisen säkerhetsinformation till statsledningen och andra myndigheter till stöd för beslutsfattandet.

En av Skyddspolisens uppgifter är att avslöja, bekämpa och för bygga följderna av främmande länders nätverksspionage i Finland. Förutom statsförvaltningen utsätts också företag för cyberspionage. I arbetet med att bekämpa cyberspionage samarbetar Skyddspolisen både med nationella och internationella samarbetspartners. Man samarbetar både med myndigheter och med näringslivet.

Skyddspolisen strävar efter att förebygga cyberspionage genom ett samarbete med intressentgrupper, där man strävar efter att öka kunskapen om cyberspionage. Bland annat utbildar man företag som upprätthåller kritisk infrastruktur och försörjningsberedskap.

Telefonnumret till Skyddspolisens växel är 0295 48013 och e-postadressen är suojelupoliisi@supo.fi.

Dataombudsmannens byrå

Dataombudsmannen är en nationell tillsynsmyndighet som övervakar efterlevnaden av dataskyddslagstiftningen. Dataombudsmannens uppgifter är bland annat att övervaka efterlevnaden av dataskyddslagstiftningen och övriga lagar om behandlingen av personuppgifter, främja medvetenheten om risker, bestämmelser, säkerhetsåtgärder, skyldigheter och rättigheter som hänför sig till behandlingen av personuppgifter, utföra utredningar och granskningar och påföra administrativa påföljder för brott mot dataskyddsförordningen.

Du kan göra en anmälan till dataombudsmannen om en personuppgiftsincident på adressen https://tietosuoja.fi/sv/anmalan-om-personuppgiftsincident.

Försörjningsberedskapscentralen och pooler

Försörjningsberedskapscentralen (FBC) är en institution inom arbets- och näringsministeriets förvaltningsområde som har i uppgift att planera och operativt genomföra upprätthållandet och utvecklingen av landets beredskap. Försörjningsberedskapscentralens uppgifter är att samordna näringslivets och den offentliga förvaltningens samarbete inom försörjningsberedskap, ha hand om statens säkerhetsupplag samt sköta den obligatoriska upplagringen och skyddsupplagringen, trygga kritisk varu- och tjänsteproduktion samt följa med den internationella utvecklingen och hålla kontakten med utländska myndigheter och organisationer.

Poolerna svarar för den operativa beredskapen i egenskap av organ som fungerar under näringslivets ledning. Deras uppgift är att tillsammans med företag inom branschen följa upp, utreda, planera och förbereda åtgärder för att utveckla beredskapen inom respektive bransch. Digipooli är ett samarbetsorgan för IT- och IT-nätverksbranschen och myndigheterna. I verksamheten deltar branschens företag och olika myndigheter. I poolen ingår viktiga tjänsteleverantörer inom informationsteknik, program- och apparatleverantörer, företag inom informationssäkerhet och teleföretag. De viktigaste myndigheterna är Traficom, Huvudstaben och Försörjningsberedskapscentralen.

För mer information om cyber-säkerhet, kontakta oss via:
cert@traficom.fi

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

traficom.fi

TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret