Transport- och kommunikationsverket
Cybersäkerhetscentret

Stärkande av cybersäkerheten i finländska organisationer

Anvisningar för ledningen och sakkunniga

Cybersäkerhetscentret

Traficoms
publikationer

8/2022

Innehållsförteckning

Den internationella situationen påverkar oundvikligen också den digitala världen och beredskapen inför cyberhot. Det är viktigt att organisationernas ledning och sakkunniga granskar och aktivt upprätthåller sina skyddsrutiner i anknytning till cybersäkerheten.

Denna anvisning gäller organisationens digitala tjänster. Med digitala tjänster avses alla datasystem och dataförbindelser som organisationen använder internt i sin verksamhet och genom vilka organisationen tillhandahåller tjänster för sina kunder.

Cyberstörningar är vanliga i det digitala samhället. Organisationernas egna system kan attackeras, men de kan också bli indirekta föremål för angrepp genom sina underleverantörer, partner eller kunder, eller så kan de bli utsatta för skada som en helt utomstående part till exempel när ett skadligt program sprids okontrollerat.

Denna anvisning är avsedd för alla finländska organisationer för att stärka cybersäkerheten. Anvisningarna begränsas inte enbart till det beredskapsbehov som den internationella situationen i början av 2022 medför, utan de kan också användas för att förbättra organisationens cybersäkerhet i allmänhet.

Läs även:

Cybersäkerhet och styrelsens ansvar

Guide för cybersäkerhet i små företag (på finska)

Ledning av cybersäkerhet

1 Observera förändringarna i hotbilden för cybersäkerheten

Varje organisation borde betrakta den förändrade hotbilden angående cybersäkerheten och hur den påverkar organisationens egen verksamhet. I sista hand är det ledningen som ansvarar för cybersäkerheten.

Cybersäkerhetscentret uppmanar organisationerna att:

- reservera tillräckliga resurser för att trygga cybersäkerheten och vidta nödvändiga åtgärder. I detta sammanhang är det också viktigt att beakta ledningens anträffbarhet för att kunna fatta kritiska beslut.
- granska vilka digitala tjänster organisationen har med tanke på organisationens kärnfunktioner som måste skyddas, samt om de åtgärder som finns för att skydda dem är aktuella och uppdaterade. I åtgärderna ska organisationens behov av såväl risk- och kontinuitetshantering som fysiska säkerhetsarrangemang beaktas.
- följa cybersäkerhetssituationen genom att ta del av myndigheternas, i synnerhet Transport- och kommunikationsverkets Cybersäkerhetscenters, meddelanden och lägesbildsprodukter, samt på eget initiativ.

Ytterligare information:

Prenumerera på våra nyhetsbrev!

Bekanta dig med våra anvisningar

Cybersäkerhet och styrelsens ansvar

2 Definiera era affärsverksamhetskritiska miljöer

Organisationens ledning ska identifiera de processer som är kritiska för organisationens verksamhet samt de digitala tjänster och den dataegendom som processerna kräver. Organisationens ledning samt de sakkunniga och partner som ansvarar för organisationens tjänster ska ha en enhetlig uppfattning om denna helhet.

En cyberstörning kan påverka flera tjänster som är nödvändiga för organisationen samtidigt. Återställandet av dessa tjänster ska basera sig på en plan som har fastställts, dokumenterats och övats i förväg. Även tjänsternas inbördes prioritetsordning ska vara klar för alla parter.

Organisationsledningen ska vara beredd på att organisationens verksamhet kan avbrytas t.ex. på grund av ett utpressningsprogram eller ett skadeangrepp som enbart syftar till att förstöra uppgifter. I en sådan situation kan verksamhetens kontinuitet endast säkerställas med hjälp av uppdaterade säkerhetskopior som går att återställa.

Kontroll över cybersäkerheten

3 Skydda era affärsverksamhetskritiska miljöer

Angriparna strävar efter att hitta de digitala tjänster som är kritiska för organisationens verksamhet och få tillgång till dem. Ofta utnyttjar angriparna i dessa fall informationssäkerhetsbrister på primär nivå.

Organisationerna ska se till att dessa hot bekämpas genom omsorgsfullt informationssäkerhetsarbete. Hot ska bekämpas genomgripande i såväl organisationens egna digitala tjänster som sådana tjänster som organisationens partner ansvarar för.

I detta kapitel har vi samlat sådana väsentliga åtgärder som vi uppmanar organisationerna att fästa uppmärksamhet vid.

Åtgärderna behöver inte vidtas i den listade ordningen, utan varje organisation ska granska och prioritera åtgärderna utifrån sina egna utgångspunkter.

Ytterligare information:

Så här skyddar du dig mot dataintrång

3.1 Använd multifaktorsautentisering

Organisationens samtliga digitala tjänster som är tillgängliga via det offentliga nätet och som kräver inloggning ska alltid använda multifaktorsautentisering (MFA, 2FA). Detta gäller såväl organisationens egna tjänster som de tjänster som tillhandahålls av externa partner.

Om det av någon anledning inte är möjligt att använda multifaktorsautentisering, ska systemet skyddas på något annat sätt genom att förhindra direkt användning av systemet via det offentliga nätet.

Ytterligare information:

Goda tips för att skydda dina konton

3.2 Installera informationssäkerhetsuppdateringar utan dröjsmål

Uppdateringar som gäller informationssäkerhet ska installeras utan dröjsmål. Detta gäller i synnerhet alla digitala tjänster som är tillgängliga via det offentliga nätet.

Tidsfönstret från att en sårbarhet hittas till att den börjar utnyttjas av brottslingarna i stor skala har ständigt blivit kortare. Det räcker inte längre med att installera uppdateringarna en gång i månaden, utan organisationen ska vara beredd att på basis av sina riskbedömningar reagera på uppdateringsbehoven senast inom några dagar.

Brottslingarna försöker också utnyttja sårbarheterna hos de terminaler som används. Därför ska särskilt apparaternas operativsystem, kontorsprogramvaror och webbläsare alltid uppdateras utan dröjsmål. För dessa fall rekommenderas införande av automatiska uppdateringar. Om uppdateringarna för organisationens terminaler administreras centraliserat är det viktigt att användarna tvingas att installera åtminstone kritiska uppdateringar senast inom en vecka.

Organisationen ska följa alla sårbarheter som är väsentliga med tanke på organisationens verksamhetsmiljö och bedöma deras betydelse för kontinuitetsriskerna i organisationens egen verksamhet. För att följa upp viktiga uppdateringar kan det vara till hjälp att veta att många tillverkare publicerar sina uppdateringar månatligen på s.k. patchtisdagar eller uppdateringstisdagar. Patchtisdag är vanligtvis den andra tisdagen i månaden.

Ytterligare information:

Cybersäkerhetscentret – Sårbarheter

Vulnerability Notes Database

Mitre Common Vulnerabilities And Exposures (CVE)

NIST National Vulnerability Database (NVD)

ICS-CERT Alerts (automatiseringsmiljöer)

3.3 Säkerställ säker datakommunikation

Organisationen ska utifrån sin egen verksamhet definiera ramarna för behövlig och normal datakommunikation i organisationens nät. Blockera all onödig datakommunikation med hjälp av brandväggar i organisationens datakommunikationsnät. Utöver den inkommande datakommunikationen ska också den utgående kommunikationen begränsas till sådan kommunikation som är nödvändig för organisationens verksamhet.

Det som särskilt ska beaktas är att det inte ska vara möjligt att kommunicera mellan organisationens nät och det allmänna nätet med ett dataöverföringsprotokoll som man vet att är sårbart eller används av brottslingar.

Inga icke-krypterade protokoll eller protokoll som har kända sårbarheter ska tillåtas från det offentliga nätet. Också då det gäller organisationens interna nät rekommenderas att man övergår till användning av krypterade protokoll i den mån det är möjligt.

I fråga om datakommunikationssäkerhet bör man också beakta servrarna och terminalerna och med hjälp av applikationsbrandväggar endast tillåta sådan datakommunikation som är nödvändig för att de applikationer som används ska fungera på ett ändamålsenligt sätt. Detta gör det också svårare för eventuella angripare som fått tillgång till organisationens nät att framskrida från en miljö till

en annan. Det här målet kan vidare stödjas genom nätverkssegmentering, dvs. genom att dela upp datanätverket i sektioner.

Ytterligare information:

NCSC-UK - Preventing Lateral Movement

NCSC-IE - Ingress & Egress Filtering

Shadowservers list över vanliga protokoll som utnyttjas av brottslingar

NSA - Network Infrastructure Security Guidance

Känner du till lateralt intrång (del 1)

Känner du till lateralt intrång (del 2)

3.4 Skydda era system mot skadliga program

Ett skadligt program som hamnar i organisationens miljö utgör en betydande risk för kontinuiteten i organisationens verksamhet. Det är ytterst viktigt att sörja för omfattande och uppdaterad bekämpning av skadliga program. Bekämpningen ska täcka organisationens alla digitala tjänster, servrar och terminaler.

Endast funktionsdugliga datasäkerhetskontroller kan skydda organisationen. Datasäkerhetskontrollernas funktion ska granskas regelbundet. Särskilt ska man se till att datasäkerhetsprodukterna har installerats i alla system och konfigurerats korrekt. Vidare ska man se till att produkterna använder uppdaterade identifieringsuppgifter och är funktionsdugliga.

Alla inkommande och utgående filer i organisationens system ska kontrolleras för skadliga program. Bekämpningen av skadliga innehåll ska beaktas också vid organisationens olika integrationsgränssnitt.

För terminaler ska man i den mån det är möjligt införa kontroller som skyddar mot skadliga länkar.

Det är viktigt att reagera på larm från terminaler eller servrar utan dröjsmål. Den enhet som larmet berör ska avskiljas från organisationens nät och undersökas omsorgsfullt, eftersom ett larm kan tyda på ett kommande intrångsförsök. Övervakningsloggarna ska kontrolleras regelbundet även om de inte ger några larm.

Cybersäkerhetscentret är intresserat av skadliga program som trängt in i organisationers system. Ni kan skicka information om skadliga program och om exempel på dem till oss genom att följa anvisningen på vår sida, se länken nedan.

Ytterligare information:

Förmedla e-post och prov till Cybersäkerhetscentret

Microsoft – Macro malware

3.5 Förbered er på överbelastningsangrepp

Överbelastningsangrepp sker varje dag på nätet. I ett typiskt överbelastningsangrepp skapas rusning i en tjänst på konstgjord väg, till exempel genom att fylla upp kanalen för internetanslutningen som tjänsten använder eller orsaka så mycket processbelastning på någon av enheterna i servicekedjan att

tjänsten stannar (denial of service, DoS). Förutom en server kan också till exempel en brandvägg bli en flaskhals.

Organisationen ska bedöma vilka av dess digitala tjänster som kan bli föremål för ett överbelastningsangrepp som stör verksamheten.

- Vilka tjänster ska fungera också i en belastningssituation?
- Hur länge kan ett överbelastningsangrepp pågå utan att verksamheten störs för mycket?

Effektiv bekämpning av överbelastningsangrepp kan kräva sådan expertis och utrustning som normalt inte står till organisationens förfogande. Om det är viktigt för organisationen att en viss tjänst fungerar, ska eventuella störande undantagssituationer beaktas redan i planeringen av genomförandet av tjänsten. Minimikravet är att det finns kännedom om var och hur snabbt det är möjligt att få experthjälp ifall den behövs.

Cybersäkerhetscentret är intresserat av överbelastningsangrepp mot organisationer. Ni kan anmäla angrepp till oss med blanketten på vår webbplats.

Ytterligare information:

Tips för att förebygga överbelastningsangrepp (på finska)

3.6 Skydda också molntjänsterna

Er organisation använder sannolikt också olika slags molntjänster. Det är viktigt att se till att alla datasäkerhetskontroller som är nödvändiga för organisationens verksamhet har tagits i bruk också för molntjänsternas del. Molntjänsternas standardinställningar är inte alltid tillräckliga med tanke på organisationens datasäkerhet.

Då det gäller externa molntjänster är det oftast leverantören som har ansvar för infrastrukturens säkerhet. Observera dock att det alltid är slutkunden som ska se till att informationen i molntjänsten är skyddad. Även om det praktiska arbetet utförs av en annan part ska organisationen ha kontroll över informationssäkerheten i anslutning till det. Organisationen ska bestämma och ge anvisningar om hur dess uppgifter ska skyddas och behandlas samt hurdana kontroller som ska tas i bruk i molntjänsterna för att skydda uppgifterna.

Ytterligare information:

Cybersäkerhetscentret – Säkerhetskriterier för molntjänster (PiTuKri)

Azure security best practices and patterns

AWS - Best Practices for Security, Identity, & Compliance

Google Cloud security best practices center

Skydd mot nätfiske och dataintrång i Microsoft Office 365

3.7 Säkerställ säkra distansförbindelser

Under coronapandemin har nästan alla organisationer varit tvungna att tillämpa nya lösningar för distansförbindelser. Brottslingar utnyttjar aktivt informationssäkerhetsbrister i anknytning till distansförbindelser.

Varje distansförbindelse innebär oundvikligen också en högre cybersäkerhetsrisk för organisationen. Därför ska organisationen allra först bedöma om de befintliga

distansförbindelserna överhuvudtaget fortfarande behövs. Det är bra att fundera på följande frågor:

- Är organisationen säkert medveten om alla former av distansförbindelser den använder för personalens eller partners behov?
- Är alla förbindelserna fortfarande nödvändiga med tanke på organisationens verksamhet?
- Behöver hela personalen eller alla partner distansförbindelser, eller räcker det t.ex. med att erbjuda dem endast till sådana aktörer som sysslar med jourarbete?
- Om organisationen använder distansförbindelser från externa partner i organisationens egen miljö, har risken för intrång genom dessa förbindelser beaktats tillräckligt bra?

Till den del distansförbindelserna anses vara nödvändiga ska organisationen säkerställa deras informationssäkerhet. Beakta följande åtgärder:

- Det ska granskas om lösningen för distansförbindelsen överhuvudtaget är tillräckligt säker för ändamålet och om den omfattas av tillverkarens säkerhetsuppdateringar.
- Sårbarheterna som gäller den produkt som används för att tillhandahålla distansförbindelsen ska följas upp och uppdateringarna installeras utan dröjsmål, något som gäller både servern och terminalerna.
- Lösningen för distansförbindelser ska ha konfigurerats så att den är säker (t.ex. multifaktorsautentisering) och endast sådana funktioner som är nödvändiga för organisationens verksamhet ska vara i bruk.
- Användarkonton som utnyttjar distansförbindelser ska upprätthållas aktivt och sådana konton som blivit onödiga (t.ex. p.g.a. ändringar i personalen) avslutas utan dröjsmål.
- Användningen av distansförbindelser ska övervakas och uppgifter om dem samlas in i en omfattande övervakningslogg. Organisationen ska ha direkt tillgång till organisationens egna loggdata i anknytning till distansförbindelser, även om själva lösningen upprätthålls av en extern partner.
- Alla distansförbindelserna ska ha dokumenterats och dokumentationen ska vara uppdaterad.

Ytterligare information:

CISA & NSA - Selecting and Hardening Remote Access VPN Solutions

3.8 Säkerställ säkerhetskopiering

Säkerhetskopior ska skapas regelbundet av alla uppgifter som är viktiga för organisationens verksamhet. Utöver affärsinformation ska säkerhetskopieringen även omfatta olika systeminställningar. Säkerhetskopiorna ska kunna användas för att återställa verksamheten också i en situation där organisationens hela datatekniska miljö måste ominstalleras.

Det är också viktigt att fästa uppmärksamhet vid hur säkerhetskopiorna skyddas. Det är viktigt att en aktör som har trängt in i miljön inte har tillgång till säkerhetskopiorna för att förstöra dem eller stjäla information med hjälp av icke-krypterade säkerhetskopior. När säkerhetskopior skapas lönar det sig att iaktta den s.k. 3-2-1-regeln. Det innebär att informationen har lagrats på minst tre

platser, den finns i minst två olika anordningar eller medier, och en säkerhetskopia finns på en helt separat plats.

Återställandet av säkerhetskopiorna ska testas regelbundet. På det sättet kan man försäkra sig om att de går att återställa och att det även finns fungerande säkerhetskopior av nödvändiga systeminställningar.

Ytterligare information:

Avancerade utpressningsangrepp har blivit vanligare – se upp för att inte bli utsatt!

Offline backups in an online world

Small Business Guide: Cyber Security

CISA – Stop Ransomware

NCSC-UK – Mitigating malware and ransomware attacks

3.9 Kontrollera vilka av era tjänster som syns i det offentliga nätet

Brottslingar söker kontinuerligt sådana organisationstjänster på webben som de kan utnyttja. Ibland är en organisation inte medveten om vilka av dess tjänster som är fritt tillgängliga på internet.

En tjänst som endast är avsedd för organisationens interna bruk kan hamna i det offentliga nätet av misstag eller t.ex. på grund av ett konfigurationsfel på brandväggen. Därför rekommenderas det att man med jämna mellanrum kontrollerar om organisationens uppfattning motsvarar verkligheten.

På webben finns olika fritt tillgängliga sökmotorer som gör det enkelt att exempelvis ta reda på vilka servrar som är kopplade till organisationens domännamn eller vilka tjänster de tillhandahåller.

Ytterligare information:

Shodan

DNSdumpster.com

3.10 Ta hänsyn till risker som trådlös teknologi medför

Flera organisationer använder också olika slags trådlösa informationsöverföringssätt som baseras på radiovågor som utbreder sig fritt. Ifall sådana informationsöverföringssätt utnyttjas i samband med organisationens kritiska funktioner är det väsentligt att också beakta hanteringen av de risker som särskilt anknyter till trådlös informationsöverföring.

Då det gäller trådlös teknologi finns det alltid en ökad risk för avlyssning och förvrängning av signalen samt eventuella avbrott i tillgängligheten till följd av oavsiktliga eller avsiktliga störningar.

Trådlösa telekommunikationsnät

Organisationen ska beakta riskerna med trådlösa telekommunikationsteknologier för dess kritiska processer:

- Ingen telekommunikationsförbindelse som är central för verksamheten får stödja sig enbart på trådlös teknik. Det ska alltid även finnas ett alternativt sätt att sörja för förbindelsen. Funktioner som är kritiska för organisationens affärs- eller annan verksamhet ska inte byggas på s.k. tillståndsfri radioutrustning på gemensamma frekvensområden där risken

för störningar är betydligt större än med frekvensområden där verksamheten baserar sig på frekvensplanering.

- Krypteringen av telekommunikationen får aldrig baseras enbart på den kryptering av radiokommunikation som möjliggörs av den trådlösa teknologin, utan den ska alltid kompletteras med en tillräckligt stark kryptering som omfattar förbindelsen från start till slut.

- Då det gäller terminaler och deras mobila anslutningar ska det beaktas att ett offentligt WLAN-nät eller ett mobilnät som tillhandahålls av en utländsk operatör inte nödvändigtvis alltid är säkert. Om dessa efter övervägande ändå måste användas, ska terminalutrustningen vara försedd med en VPN-förbindelse som förvaltas av organisationen.

Positions- och tidsdatatjänster

Satellitpositioneringssystemets (GNSS) bastjänster omfattar positions- och tidsdata som är öppna för alla. Tillgång till dessa uppgifter tas ofta för given. Organisationen ska utreda vilka konsekvenser det skulle innebära för dess verksamhet om uppgifternas tillförlitlighet försvagades eller om tillgången till dem avbröts för en längre tid, dvs. för minst flera dagar:

- Exakt och tillförlitlig positionsdata utgör en viktig del av exempelvis utvecklingen av intelligenta transport- och lägesbildssystem där koordineringen av olika funktioner bygger på data om personernas eller anordningarnas läge i området. Till exempel optimerar logistikföretagen användningen av materielen utifrån positionsdata. Inom luftfarten, sjöfarten och järnvägstrafiken utnyttjas positionsdata aktivt till stöd för den operativa verksamheten.

- Tidsdata utnyttjas i stor utsträckning i bland annat telekommunikations-, tele-, televisions- och energiöverföringsnät för synkronisering av funktionen hos olika systemdelar.

Vad beträffar positionsdata kan funktionssäkerheten förbättras genom att anlita flera GNSS-system, t.ex. en kombination av europeiska Galileo och amerikanska GPS, och mottagning på flera frekvenser. GNSS-mottagningens tolerans för störningar kan eventuellt förbättras också med hjälp av olika slags antennlösningar. Vissa GNSS-mottagare är också försedda med programmerade egenskaper som förbättrar mottagarens tolerans för störningar och som kan aktiveras separat. Positionsdata kan också kompletteras med mobilnätets lokaliseringstjänster.

Inom sjöfarten och båttrafiken är det viktigt att säkerställa tillgången till behövligt kartmaterial och manuella navigeringssystem.

För att säkerställa tidsdata är det också möjligt att utnyttja flera GNSS-system. Det rekommenderas dock att det även finns ett reservsystem som baserar sig på trådbunden teknik eller ett lokalt klocksystem.

Ytterligare information

Säker användning av anordningar anslutna till internet (på finska)

Säker användning av Bluetooth på smarta enheter

Nuläget och utvecklingsutsikterna för satellitpositionering (på finska)

Anmälan om radiostörningar

Observera, reagera och sörja för verksamhetens kontinuitet

4 Observera och analysera händelser

Organisationen ska trygga förmågan att upptäcka informationssäkerhetsincidenter i sina kritiska miljöer. Loggdata ska samlas in om sådana anordningar, programvaror och datalager som angripare kan utnyttja. Loggdata krävs för att kunna utreda vad som har hänt, varför och när.

Kravet på loggning fastställs enligt hur kritiska de objekt som ska skyddas är. Ju större potentiell inverkan det skyddade objektet har om det äventyras, desto mer logguppgifter ska organisationen samla in om det.

Logguppgifterna ska skyddas mot eventuella angripare. Loggarna ska sparas på ett säkert sätt någon annanstans än i den övervakade miljön så att angriparen inte kan ändra dem.

Organisationen ska följa upp de insamlade logguppgifterna för att få en tydlig allmän bild av den operativa verksamhetens och cybersäkerhetens tillstånd. För närvarande ska särskilt tecken på följande angelägenheter följas i logguppgifterna:

- Onormala händelser i inloggningsloggar för användardatabaser och katalogtjänster (t.ex. Active Directory eller Azure AD). Exempel på dessa är skapande av nya användarkonton, ökning av användarrättigheterna eller inloggning från geografiskt ovanliga lägen, från ovanliga terminaler eller vid ovanliga tidpunkter.
- Ovanliga adresser, protokoll, trafikmängder eller tidsmässigt ovanliga händelser i brandväggsloggar.

Ytterligare information:

Så här samlar du in och använder loggdata

NCSC-UK - Logging made easy (LME)

5 Reagera på incidenter och störningar

Organisationen ska vara beredd att omedelbart reagera på cyberincidenter eller -störningar som berör organisationens kritiska funktioner. Lämpliga ansvarspersoner eller roller ska identifieras för dessa situationer i förväg.

Det mest centrala målet med denna punkt är att begränsa incidentens konsekvenser för organisationens verksamhet och möjliggöra återställandet av verksamheten till det normala. Organisationen ska ha en färdig plan på hur man reagerar på cyberstörningar. Planen ska vara uppdaterad och täcka hela livscykeln för störningshanteringen.

Ytterligare information:

Guide för att upptäcka dataintrång (på finska)

NCSC-UK - Incident management

6 Trygga verksamhetens kontinuitet

Organisationen ska ha planer för att trygga verksamhetens kontinuitet för att kunna bevara och återställa verksamheten ifall den blir föremål för en cyberincident eller -störning.

I kontinuitetsplanerna identifieras och dokumenteras de anordningar, programvaror och datalager samt funktioner som minst krävs för att upprätthålla verksamheten.

Ytterligare information:

FBC – Kontinuitetshantering

Trygga den digitala verksamheten i en störningssituation (på finska)

7 Informera personalen

Då det gäller att sörja för cybersäkerheten har hela personalen i organisationen en viktig roll. Därför ska ledningen se till att personalen är tillräckligt medveten om cybersäkerhetens betydelse för organisationens verksamhet. Här har ledningen och kommunikationen en nyckelroll.

Personalen ska med hjälp av utbildning och kommunikation ges tillräckliga färdigheter för att möta vardagliga cybersäkerhetshot.

Därmed ska minst följande åtgärder vidtas i organisationen:

- Ledningen informerar hela personalen tydligt om cybersäkerhetens betydelse för organisationens verksamhet och om ledningens entydiga engagemang för temat.
- Personalen erbjuds regelbunden utbildning i informationssäkerhet som är tillräcklig med tanke på personalens arbetsuppgifter. Målet med utbildningen är att personalen har verktyg för att arbeta på ett tryggt sätt och beakta de vanligaste riskerna för informationssäkerheten i sitt arbete, såsom nätfiske, skadliga bilagor samt länkar.
- En kanal ordnas för personalen där den har möjlighet att rapportera inträffade och misstänkta informationssäkerhetsincidenter.

Ytterligare information:

Så här sörjer du för informationssäkerheten hemma och på arbetsplatsen

8 Rapportera inträffade och misstänkta säkerhetsöverträdelser

Cybersäkerhetscentret uppmanar organisationer att med låg tröskel meddela Centret om inträffade och misstänkta säkerhetsöverträdelser.

Anmälan kan göras helst med **blanketten** på Cybersäkerhetscentrets webbplats eller i andra hand per e-post: **cert@traficom.fi**. Om incidenten inte är akut ber vi er att kontakta oss via **cybersakerhetscentret@traficom.fi**.

Den insamlade informationen utnyttjas för att upprätthålla den nationella lägesbilden av cybersäkerheten. Vid behov kontaktar vi också den som har anmält incidenten.

En säkerhetsöverträdelse är ett brott och därför ska en brottsanmälan alltid göras till polisen. Om det också är fråga om en personuppgiftsincident ska incidenten anmälas till dataombudsmannen. Centrala försörjningsberedskapskritiska aktörer och tjänsteleverantörer ska rapportera informationssäkerhetsincidenter i sina nätverks- och datasystem också till tillsynsmyndigheten inom respektive sektor (NIS-skyldighet).

Ytterligare information:

Utredning av cyberbrott

Rapportera en it-säkerhetsincident (NIS-skyldighet)

Personuppgiftsincidenter

Förmedla e-post och prov till Cybersäkerhetscentret

Transport- och kommunikationsverket Traficom
Cybersäkerhetscentret

PB 320, 00059 TRAFICOM
tfn 029 534 5000

kyberturvallisuuskeskus.fi

ISSN 2669-8757 (internet)
ISSN 2669-8749 (print)

Transport- och kommunikationsverket
Cybersäkerhetscentret