TRAFICOM
Transport- och kommunikationsverket

Kommunikation i samband med cyberangrepp

Kriskommunikationsanvisning för organisationer

Traficoms publikationer
11/2025

Kommunikation i samband med cyberangrepp

Anvisningen som har tagits fram av Cybersäkerhetscentret vid Traficom har utarbetats i samarbete med Finansinspektionen, Centralkriminalpolisen, Kommunförbundet, Polisstyrelsen, Skyddspolisen och dataombudsmannens byrå.

Utkastversioner av anvisningen har kommenterats av mediechef Päivi Anttikoski vid SOK, CISO Ilja Ikonen från Verkkokauppa.com Abp, kommunikationsdirektör Katja Kannonlahti vid Tammerfors stad, kommunikationsdirektör Eriikka Koistinen vid inrikesministeriet, SVP (Sustainability, HSE & Communications) Kaisa Lipponen vid Paulig Oy, kommunikationsdirektör Marjo Loisa vid Institutet för hälsa och välfärd, professor i kommunikationsledning Vilma Luoma-aho vid Jyväskylä universitetets handelshögskola, kommunikationsdirektör Pipsa Lotta Marjamäki vid FPA, kommunikationsdirektör Marika Nöjd vid Tallink Silja Oy, biträdande kommunikationsdirektör Jyri Rantala vid statsrådets kansli, ledande specialsakkunnig Kimmo Rousku vid Myndigheten för digitalisering och befolkningsdata, kommunikationsdirektör Päivyt Tallqvist vid Finnair Abp, enhetschef Päivi Tampere vid Natos kompetenscentrum för strategisk kommunikation i Riga (Nato StratCom COE) samt säkerhetschef Jaakko Wallenius vid Elisa Abp.

Följande organisationer har kommenterat utkast till anvisningen: Fiskars Abp, LokalTapiola Ab, Brottsofferjouren, Telia Finland Abp och statsrådets kansli.

Vi vill tacka alla experter och organisationer för kommentarerna och stödet i arbetet med att ta fram anvisningen.

Ytterligare information: Jussi Toivanen, kommunikationschef, fornamn.efternamn@traficom.fi, Transport- och kommunikationsverket Traficom

Inledning

I och med digitaliseringen av samhället är vi allt mer beroende av tillförlitliga och informationssäkra tjänster i vår vardag. Under de senaste åren har tyvärr allt fler organisationer och individer utsatts för cyberangrepp, vilket ofta lett till dataläckage eller dataintrång.

Transport- och kommunikationsverket Traficom och Skyddspolisen har tillsammans konstaterat att hotnivån inom cybersäkerhet har ökat i Finland[1]. Orsaken är att cyberangreppen som riktas mot finländska organisationer är mer målinriktade och skräddarsydda än tidigare. Angriparna väljer medvetet sina mål och utformar sin angreppsstrategi organisationsspecifikt. Dessutom är de beredda att ständigt testa nya metoder vid intrångsförsök om en metod inte lyckas.

Praktiska erfarenheter av cyberangrepp har visat att organisationer måste satsa på kommunikation och att dess betydelse och roll i ledningen inte får förbises. Kommunikationsinsatserna måste vara öppna, regelbundna, målgruppsanpassade och proaktiva.

Människan – medarbetaren, kunden eller samarbetspartnern – är den som drabbas av ett cyberangrepp. Ett cyberangrepp väcker oro, osäkerhet och rädsla. Den som förlorat sina pengar eller känsliga uppgifter kan drabbas av allvarliga ekonomiska, sociala, psykiska och hälsomässiga konsekvenser. Därför är det viktigt att sätta människan i centrum vid hantering och kommunikation i cyberrelaterade situationer. Människan får inte glömmas bort bakom tekniska aspekter såsom servrar, VPN-anslutningar, routrar, bitar och botar.

Kommunikation om cyberangrepp har särskilda kännetecken som är viktiga att känna till. En särskild kommunikationsutmaning är att lägesbilden och förståelsen ofta förändras under utredningens gång. Företag eller organisationer tvingas därför ofta kommunicera med bristfällig eller föränderlig information, ibland under en längre tidsperiod. I alla situationer är de viktigaste målgrupperna de personer vars personuppgifter kan ha äventyrats samt den egna personalen. Det är också viktigt att komma ihåg att informera den som drabbats av en personuppgiftsincident på det sätt som dataskyddslagstiftningen kräver.

[1] Hotnivån mot cybersäkerhet har förblivit förhöjd - antalet riktade angrepp har ökat | Traficom

I denna anvisning berättar vi om olika cyberangrepp samt om metoder och tillvägagångssätt som används av brottslingar. Vi ger även tips om hur man kommunikationsmässigt förbereder sig och hur man bör kommunicera under och efter ett cyberangrepp.

Guiden är avsedd för organisationers ledning, säkerhets- och kommunikationsexperter samt de experter som ansvarar för lägesbild och beredskap. Vid ledning, hantering och kommunikation av cybersituationer är det viktigt att information om det inträffade och planerade eller genomförda åtgärder överförs smidigt mellan ledning, kommunikation och lägesbildsfunktion.

2 Cyberbrottslighet och metoder för påverkan

Cyberbrottslighet är kriminell verksamhet som sker via digitala system och nätverk. Den kan omfatta många olika brott, såsom identitetsstölder, dataintrång, dataskyddsbrott, nätfiske (phishing), spridning av skadliga program och utpressningsprogram. Cyberbrottslighet är internationell och kommersiell verksamhet. Den drivs av möjligheten till betydande ekonomisk vinning och den låga risken att åka fast. Om man jämför de globala ekonomiska vinsterna från brottslighet med länders nationalekonomier, skulle det utgöra världens tredje största ekonomi efter USA och Kina. För att genomföra ett cyberangrepp behöver man inte själv behärska tekniken eller teknologin, utan attacken kan beställas som en nyckelfärdig tjänst från brottslingar på nätet (Crime-as-a-Service).

Konsekvenserna av cyberangrepp kan vara allvarliga för individer, organisationer och stater. De kan leda till ekonomiska förluster, skada anseendet och till och med utgöra hot mot nationell säkerhet. De kan även underminera förtroendet för institutioner och samhällsfunktioner.

Vid cyberangrepp och cyberpåverkan är det lätt att fokusera på det tekniska. Det är dock viktigt att förstå att det framför allt handlar om social och psykologisk påverkan. Det handlar om metoder som förenar cyberpåverkan med informationspåverkan.

Cyberbrottslingar och andra illvilliga aktörer riktar sina påverkningsförsök mot oss som individer. Brottslingarna utnyttjar våra mänskliga svagheter, såsom behovet att bli omtyckt eller att snabbt agera under stress och undvika misstag. I praktiken kan det yttra sig som att nätbrottslingar försöker få oss att lämna ut information eller öppna en bilaga som innehåller ett skadligt program i ett e-postmeddelande genom att hänvisa till brådska. ”Du har inte betalat vår faktura, agera nu för att undvika utsökning. Klicka på länken och betala omedelbart.” Förutom den stressande eller pressande tonen kan budskapet också vara lockande: ”Du har betalat fakturan två gånger, vi återbetalar dig.”

Utpressning och hot är också medel som brottslingar och illvilliga aktörer använder. ”Om du inte agerar på ett visst sätt kommer vi att offentliggöra känslig information om dig eller ditt företag.” Syftet är att få den drabbade att agera mot sina egna eller sin organisations intressen.

Cyberangrepp kan användas som metoder för informationspåverkan. Syftet kan vara att skapa osäkerhet i samhället eller att underminera allmänhetens förtroende för organisationer och det digitala samhället i stort. Cyberangrepp är iögonfallande och kan enkelt få publicitet.

Motivationen bakom angreppet avgör om det handlar om skadegörelse, ekonomisk vinning eller verksamhet som ska klassas som informationspåverkan. Det kan dock vara svårt att avgöra den bakomliggande avsikten. Ur informationspåverkansperspektiv är det viktigt att inse att ett offentliggjort cyberangrepp alltid påverkar informationsmiljön.

Metoder för informationspåverkan kan också användas för att stödja cyberangrepp, till exempel genom att avleda uppmärksamheten, dölja eller iscensätta aktören. I dagens digitala samhälle är cyber- och informationspåverkan tätt sammankopplade och förstärker varandra. Om ett cyberangrepp lyckas underminera människors förtroende för en organisation eller samhället i stort kan återhämtningen vara svår.

Inom informationssäkerhet är det viktigt att beakta användningen av cybermetoder som en del av informationsoperationer. Teknologisk utveckling, såsom deepfake-teknik, erbjuder allt mer effektiva, kraftfulla och skräddarsydda verktyg för social manipulation. Lögner kan maskeras på ett mer trovärdigt sätt och blir svårare att avslöja. Brottslingar och andra illvilliga aktörer kan exempelvis använda AI-applikationer för att skapa virtuella kopior av personer i ledande positioner. Dessa kopior kan i video se ut och låta som de verkliga personerna, men säga eller göra saker de aldrig gjort eller skulle göra.

En person som ser eller hör en video- eller ljudinspelning kanske inte inser att det är en förfalskning som skapats med deepfake-teknik, utan tror att den är äkta. Det har redan rapporterats fall i världen där videosamtal i realtid har manipulerats med falska klipp. Det här är inte science fiction utan en verklighet som organisationer måste förbereda sig på. Den snabba tekniska utvecklingen förbättrar kvaliteten på dessa förfalskningar och sänker kostnaden för den nödvändiga tekniken.

Cyberangepp är också ett medel för hybridpåverkan och spionage. Hybridpåverkan avser fientlig, planerad och kontinuerlig verksamhet som bedrivs av en främmande stat mot en annan stat genom att utnyttja svagheter hos mållandet. Syftet med hybridpåverkan är bland annat att försvaga samhällets funktionsförmåga och beslutsfattande. I sådan verksamhet används politiska, diplomatiska, ekonomiska och militära medel men också cyber- och informationspåverkan samt spionage.

I vardagen visar sig påverkan som störningar i samhällets funktioner, cyberangrepp eller spridning av desinformation. Framgångsrik påverkan syns som ökad samhällelig polarisering och rädsla, samt som minskat förtroende för samhället. Det är viktigt att påminna om att majoriteten av cyberangreppen fortfarande handlar om ekonomisk vinning för brottslingar som alltså inte har något att göra med statlig hybridpåverkan eller spionage.

1 Fenomen i cybervärlden

Vårt digitala samhälle är beroende av olika elektroniska tjänster och informationssystem. Därför påverkar störningar i dessa betydligt vår vardag, organisationers verksamhet och samhällets funktion i stort. I ett digitalt samhälle lagras även sekretessbelagd information i stor utsträckning i digitala informationssystem, vilket gör dem till intressanta mål för cyberspionage.

Cyberstörningar är situationer där organisationers digitala tjänster eller system inte fungerar normalt till exempel på grund av ett tekniskt fel.

Ett **cyberangrepp** är skadegörelse eller störning som kan riktas mot till exempel informationsnät, system, enheter eller digitalt lagrad information, det vill säga data. Även nätfiske direkt från människor är ett cyberangrepp. I detta avsnitt presenterar vi närmare olika fenomen i cybervärlden och metoder som brottslingar använder för att genomföra angrepp mot organisationer. Kunskap om dessa fenomen och metoder är viktig vid planering och genomförande av motåtgärder och kommunikation.

Brottslingar, spioner och andra illvilliga aktörer har tillgång till olika taktiker för cyberangrepp. Angreppen kan variera från enkla överbelastningsangrepp som stör en organisations webbsidor eller tjänster till allvarligare former såsom dataintrång där känslig information stjäls, eventuellt läcks till offentligheten eller skadas.

Även **utpressningsprogram** är vanliga. De kan låsa en organisations informationssystem eller hindra åtkomst till kritisk information genom att kräva lösen. Sådana angrepp kan orsaka betydande ekonomiska skador och skada organisationers och individers rykte.

Cyberangrepp har utöver **ekonomiska effekter** även alltid **mänskliga och psykosociala konsekvenser**. Till exempel kan en anställd i en organisation som drabbats av ett dataintrång känna rädsla och ångest eftersom det inte är klart vilken information som stulits och hur den kan användas mot dem. Dataintrång innebär alltid ett intrång i de anställdas och kundernas integritet. Behovet av information bland olika målgrupper efter ett cyberangrepp är stort.

1.1 Utpressningsprogram

1.1.1 Vad handlar det om?

Ett utpressningsprogram är ett program som hindrar normal användning av en enhet eller tjänst och kräver att offret betalar lösen till brottslingarna. Denna typ av skadligt program kallas även för utpressningstrojan. Utpressningsprogram (eng. ransomware) krypterar typiskt filer på enheten med en krypteringsalgoritm och en nyckel som endast angriparen har tillgång till. Ofta försöker angriparen också stjäla offrets information.

Efter att filerna har krypterats eller skärmen låsts lämnar programmet vanligtvis ett meddelande till offret där det informerar om att åtkomsten kan återställas mot betalning av lösen. Betalning krävs ofta i kryptovaluta vilket gör transaktionen svårare att spåra än betalningar i traditionella valutor. Allt oftare är utpressningsprogram bara ena halvan av angreppet. Den andra halvan är stöld av information och hot om att läcka informationen för att pressa fram lösensumman.

Brottslingar sprider utpressningsprogram både slumpmässigt – till exempel via e-post – och genom riktade dataintrång. De vanligaste spridningsmetoderna är länkar och bilagor i e-postmeddelanden, förfalskade nedladdningsbara filer såsom piratkopior av betalprogram samt utnyttjande av kända sårbarheter i programvara.

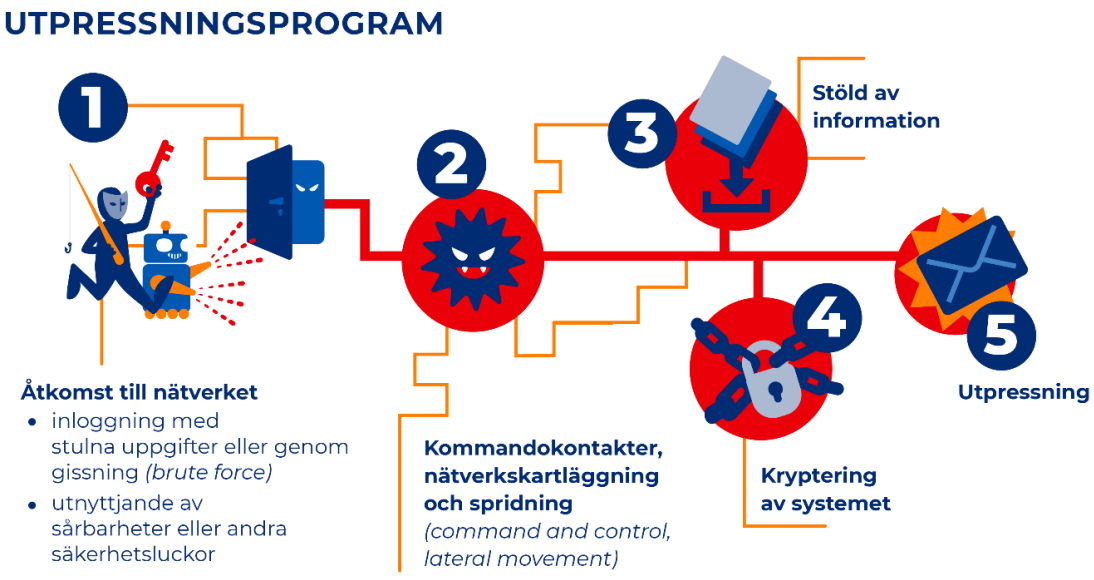

Bild 1. Utpressningsprogram (eng. ransomware) kallas även för utpressningstrojan.

1.1.2 Vilka är konsekvenserna för organisationer?

Ett utpressningsprogramangrepp kan upptäckas till exempel genom ett utpressningsmeddelande, ett larm från en informationssäkerhetsprodukt eller genom att åtkomsten till filer blockeras. De allvarligaste följderna av

ett lyckat angrepp är att användare inte längre har tillgång till informationen på den infekterade enheten. Om inga säkerhetskopior finns kan informationen vara förlorad för alltid.

För företag kan ett utpressningsprogramangrepp medföra stora ekonomiska konsekvenser. Företaget kan förlora stora summor på grund av avbrott i verksamheten och kostsamma återställningsåtgärder. Även ett slumpmässigt spritt skadligt program kan orsaka allvarliga störningar eftersom det i början ofta är oklart hur omfattande problemet är när utpressningsprogrammet upptäcks på en enhet.

Lösensummor som krävs av utpressningsprogramaktörer bör inte betalas. Att betala lösensummor uppmuntrar brottslig verksamhet att fortsätta, och det finns inga garantier för att informationen återställs eller att utpressningen upphör.

1.1.3 Att beakta i kommunikationen

Ett cyberangrepp med utpressningsprogram har allvarliga konsekvenser för organisationens ledning, dagliga verksamhet och kommunikation. Det kan bli nödvändigt att begränsa eller helt stoppa användningen av kommunikations- och ledningskanaler. Tillförlitlig informationsöverföring samt intern och eventuell extern kommunikation måste då flyttas till alternativa kanaler.

Det kan ta tid att fastställa omfattningen av skadorna från ett angrepp som genomförts med utpressningsprogram. Det är möjligt att angriparen fått tillgång till känslig information såsom anställdas personuppgifter eller affärshemligheter.

I kommunikationen under angreppets inledningsskede bör man genast förbereda sig på det värsta – att känslig information (kunduppgifter, företagshemligheter, avtal och uppgifter om anställda) läckt till brottslingar. Om personuppgifter har läckt måste organisationen komma ihåg skyldigheterna enligt den allmänna dataskyddsförordningen. Dessa beskrivs i kapitel 2.2.6 Dataskyddsskyldigheter i denna anvisning.

Även om situationen är oklar, kanske länge, kan organisationen inte låta bli att kommunicera. Informationen måste vara aktuell, lagstadgad, öppen och tillgodose målgruppernas rättigheter och behov. Ett börsbolag, det vill säga ett bolag vars värdepapper är föremål för handel, ska i sin kommunikationsplanering beakta eventuell uppkomst av insiderinformation som kan påverka marknaden och offentliggöra denna i enlighet med gällande reglering. Det handlar om att vinna och/eller återvinna avgörande förtroende för organisationens verksamhet och framtid.

Organisationen måste också förbereda sig på att brottslingarna när som helst kan bli aktiva i sin egen kommunikation, till exempel genom att publicera information om angreppet eller stulna data i sina egna kanaler. De kan också kontakta organisationens kunder eller anställda direkt och försöka utpressa dem med hjälp av den information som erhållits. Det är alltid bättre om den drabbade organisationen hinner kommunicera till sina viktigaste målgrupper först. Öppen och transparent kommunikation samt tydliga handlingsanvisningar till personal, kunder och andra intressentgrupper är avgörande.

Om organisationen har verksamhet utanför Finland måste kommunikationen och anvisningarna även nå internationella kunder och anställda. Anvisningarna måste beakta lokal reglering och myndigheters instruktioner i respektive land.

1.2 Nätfiske

1.2.1 Vad handlar det om?

Vid nätfiske försöker brottslingar få tillgång till exempelvis personuppgifter, bankkoder eller betalkortsuppgifter. Även användarnamn och lösenord som används i olika elektroniska tjänster är av intresse för både brottslingar och spioner. Brottslingar är intresserade av information som kan ge ekonomisk vinning, medan spioner söker information som kan gynna en annan stat.

I nätfiskekampanjer har brottslingar använt logotyper från välkända varumärken och organisationer, och utgett sig för att vara anställda eller ledande personer inom dessa organisationer som en del av bedrägeriet. Brottslingarna försöker ofta skapa brådska, vädja till känslor och få offret att förbise normala processer. Brottslingarna använder även betalda och sökmotoroptimerade sökresultat för att sprida sina länkar.

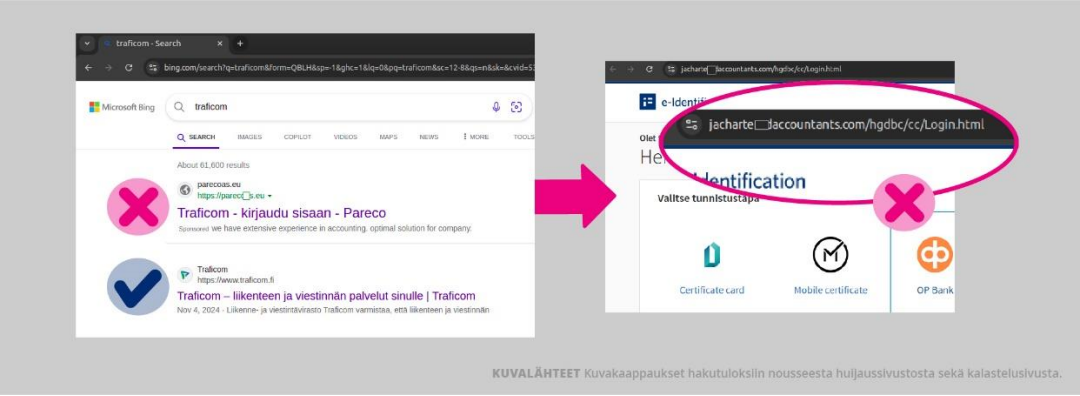

Bild 2. Vid nätfiske utnyttjar brottslingar logotyper och varumärken från välkända och pålitliga organisationer som verktyg i sina bedrägerier. Brottslingarna använder också betalda sökresultat för att sprida sina länkar.

1.2.2 Vilka är konsekvenserna för organisationer?

Vid nätfiske utnyttjar brottslingar logotyper och varumärken från välkända och pålitliga organisationer som verktyg i sina bedrägerier. Det handlar ofta om bluffmeddelanden via e-post eller sms som skickas till allmänheten. Dessa meddelanden är utformade med organisationens egna meddelandemallar, varumärken och logotyper. För organisationen utgör detta en ryktesrisk även om organisationen inte på något sätt är inblandad i den brottsliga verksamheten. Brottslingarnas verksamhet kan påverka allmänhetens förtroende för organisationen och trovärdigheten i dess egen kommunikation.

Det är viktigt att notera att denna anvisning granskar nätfiske ur perspektivet av varumärkesmissbruk. Det är dock även viktigt att komma

ihåg att organisationens egna anställda också kan vara måltavlor för denna typ av verksamhet. Nätfiske kan vara det första steget i ett utpressningsprogramangrepp.

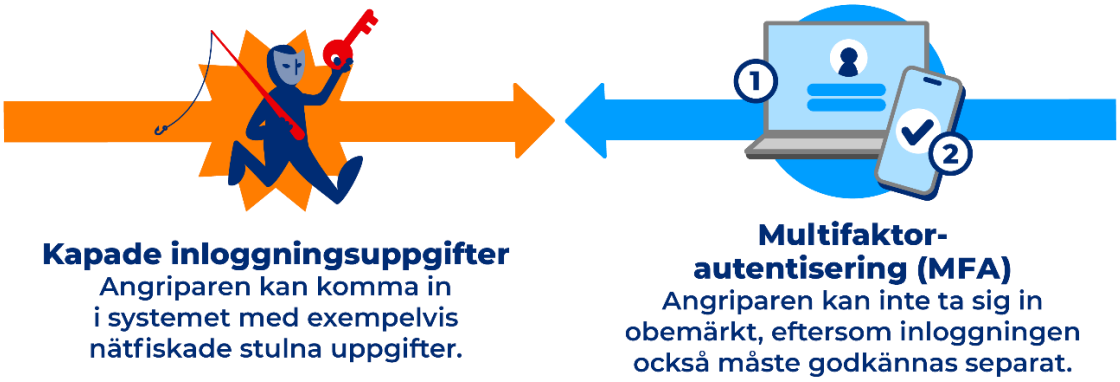

Bild 3. Inloggningsuppgifter som stulits genom nätfiske är ett av de vanligaste sätten att ta sig in i en organisations system. Multifaktorautentisering försvårar angriparens tillgång till systemen.

1.2.3 Att beakta i kommunikationen

Nätfiske i organisationens namn är ett fenomen som det är både möjligt och rekommenderat att kommunicera proaktivt om. Kunder som använder organisationens digitala tjänster kan till exempel varnas om nätfiske via en banner på webbplatsen eller genom information på organisationens sociala mediekanaler. Om organisationen ofta utsätts för nätfiske bör kommunikationen upprepas regelbundet. Organisationen kan också upprätthålla en webbsida med exempel på vanliga bedrägerier som har utförts i dess namn. Eftersom bluffar hela tiden skapas med nya adresser och profiler, är ökad allmän medvetenhet ett viktigt försvar.

Organisationen måste även vara beredd att snabbt reagera på bedrägerimeddelanden som sprids i dess eller dess ledares/anställdas namn.

Snabb respons och ökad medvetenhet hjälper till att förhindra att människor blir lurade och faller offer för brott. För organisationen handlar det också om trovärdighet och rykte. Även om organisationen inte själv är skyldig till brottet kan förekomsten av dess logotyp i samband med kriminell verksamhet minska förtroendet för den. Bedrägerimeddelanden som sprids i organisationens namn är brott där organisationen är måltavla.

1.3 Överbelastningsangrepp

1.3.1 Vad handlar det om?

Vid överbelastningsangrepp riktas stora mängder trafik mot en webbplats eller nätbaserad tjänst.

För användare syns detta så att det inte är möjligt att gå in på webbsidorna eller att sidorna laddar mycket långsamt. Överbelastningsangrepp är en enkelt genomförbar och effektfull angreppsteknik. Därför får de ofta uppmärksamhet även i medierna. Överbelastningsangreppen medför i allmänhet inte några synliga konsekvenser för användare och i värsta fall blir det närmast korta avbrott i användningen av offentliga webbtjänster.

Numera är överbelastningsangrepp särskilt vanliga som en form av hacktivism. Hacktivism är en form av cyberbrottslighet där motivet är politiskt snarare än ekonomiskt. Genom överbelastningsangrepp uttrycks missnöje med ett politiskt beslut eller annan åtgärd, och man försöker påverka informationsmiljön kring händelsen. Även kortvariga avbrott kan leda till ökad misstro hos den drabbade partens kunder och intressentgrupper samt väcka oro över om deras personliga uppgifter är säkra.

1.3.2 Vilka är konsekvenserna för organisationer?

Som metod är ett överbelastningsangrepp uppseendeväckande eftersom en otillgänglig webbsida är något mycket konkret för användaren och kan orsaka frustration om tjänsten inte är tillgänglig. Angrepp som riktas mot e-tjänster eller till exempel en webbutiks webbplats kan väcka oro hos människor om huruvida deras information är säker. Det är dock viktigt att komma ihåg att störningarna ofta är kortvariga. I praktiken lyckas sådana angrepp sällan orsaka verkliga och långvariga skador. Människors information äventyras mycket sällan vid dessa angrepp. Det handlar snarare om att ”klottra i skyltfönstret”, alltså att slå ut en webbplats eller tjänst, så kallad digital graffiti.

1.3.3 Att beakta i kommunikationen

En otillgänglig tjänst eller webbplats försvårar vardagen för kunderna och orsakar frustration, osäkerhet och oro. Det är viktigt att vara aktiv och snabb i kommunikationen. Man bör informera om vad överbelastningsangrepp är, vad som ligger bakom dem och hur de påverkar organisationens verksamhet. Det är också viktigt att informera om vilka åtgärder som vidtagits för att återställa situationen till det normala, hur länge tjänsterna eventuellt är otillgängliga och om det finns alternativa sätt

att uträtta ärenden. Det är också viktigt att meddela när överbelastningsangreppet är över och tjänsterna fungerar igen.

Om organisationens webbsidor eller tjänster är utslagna på grund av ett överbelastningsangrepp bör man noggrant följa med ifall någon aktör börjar sprida bluff- eller nätfiskemeddelanden i organisationens namn. Om organisationens kommunikationskanaler har begränsats på grund av angreppet kan en opportunistisk brottsling försöka utnyttja detta informationsvakuum genom att kapa organisationens kommunikation delvis eller helt.

Situationen kan också användas som ett medel för informationspåverkan, det vill säga för att underminera människors förtroende för organisationen eller det digitala samhället i stort.

Ett börsbolag, det vill säga ett bolag vars värdepapper är föremål för handel, ska i sin kommunikationsplanering beakta eventuell uppkomst av insiderinformation som kan påverka marknaden och offentliggöra denna i enlighet med gällande reglering.

1.4 Cyberspionage

1.4.1 Vad handlar det om?

Riktade cyberangrepp kan också vara cyberspionageoperationer som utförs av statliga aktörer eller av aktörer som agerar för en stats räkning. Målet är vanligtvis att samla in information om exempelvis en annan stats beslutsfattande eller ett företags produktutveckling. Förutom insamling av information kan cyberspionage även innebära påverkan och till och med förstörelse av informationssystem eller annan skadegörelse.

För en spionerande stat är cyberspionage ett effektivt och relativt riskfritt sätt att få tillgång till stora mängder konfidentiell information. Offret för cyberspionaget märker inte nödvändigtvis att det har blivit utsatt.

En stat kan genomföra cyberspionage till exempel genom att tränga in i informationssystem via tekniska sårbarheter. Den kan även kräva att leverantörer av utrustning eller programvara inom dess jurisdiktion samlar in data om sina utländska kunder. Även vid cyberspionage kan åtkomst erhållas genom riktat nätfiske eller andra personanpassade metoder. Det slutliga målet är att komma åt konfidentiell information.

Alla som har en betydelsefull roll eller hanterar viktig information kan vara mål för utländsk underrättelseverksamhet.

1.4.2 Vilka är konsekvenserna för organisationer?

Konsekvenserna av cyberspionage kan i värsta fall sträcka sig utanför den enskilda organisationen om information som är viktig för Finlands nationella säkerhet hamnar hos en fientlig stat. Ofta är det oklart i inledningsskedet hur långt angriparen har lyckats tränga in och vilken information som eventuellt har läckt. När statlig cyberspionage misstänks bistår myndigheterna med att utreda situationen och begränsa skadorna. Det är viktigt att omedelbart kontakta myndigheterna (Skyddspolisen, polisen eller Cybersäkerhetscentret vid Traficom), särskilt om organisationen hanterar information som kan vara av intresse för fientliga främmande makter.

1.4.3 Att beakta i kommunikationen

Cyberspionage är både ett brott som kan leda till att polisen inleder en förundersökning och en händelse som kan påverka Finlands internationella relationer. Därför måste man i kommunikationen ofta ta hänsyn till även utrikespolitiska konsekvenser. Skyldighetsfrågor avgörs i domstol, medan beslut om formell attribuering av angriparen i slutändan fattas av den utrikes- och säkerhetspolitiska ledningen utifrån myndigheternas utredningar.

Organisationen måste ändå informera sin personal och beroende på situationen även externa intressentgrupper om det inträffade. I denna kommunikation bör fokus ligga på de konkreta effekterna av händelsen samt på åtgärderna för att begränsa skadorna. Vid behov kan organisationens ledning eller kommunikationsfunktion föra en dialog med de myndigheter som utreder händelsen och komma överens om gemensamma riktlinjer för kommunikationen.

1.5 Dataintrång och informationsläckor

1.5.1 Vad handlar det om?

Dataintrång betyder olovligt intrång i ett IT-system, en tjänst eller en enhet eller olovlig användning av en applikation, till exempel ett e-postkonto, med hjälp av erhållna koder. Dataintrång begås också genom olika intrångssätt förbi säkerhetssystem, till exempel genom att utnyttja sårbarheter. Dataintrång är straffbart enligt strafflagen och även försök till dataintrång är straffbart.

1.5.2 Vilka är konsekvenserna för organisationer?

Dataintrång kan medföra till exempel ekonomisk skada, avbrott i verksamheten samt skada den drabbade organisationens rykte. Stulna uppgifter kan till exempel publiceras obehörigt eller deras innehavare kan utpressa offret genom att kräva en lösensumma. Om angriparen får tillgång till personuppgifter om organisationens anställda eller kunder, kan dessa användas till exempel i identitetsstölder, utpressning eller trakasserier.

Dataintrånget kan leda till ett dataläckage, om angriparen får tillgång till känslig information i informationssystemet. Vid en läcka kan angriparen komma över personuppgifter, faktureringsinformation, kontouppgifter, betalkortsuppgifter, företagshemligheter, personuppgifter som tillhör särskilda kategorier av personuppgifter om kunder eller enskilda anställda eller annan sekretessbelagd eller värdefull information. Om läckan omfattar personuppgifter och tröskeln enligt den allmänna dataskyddsförordningen överskrids, måste händelsen anmälas till dataombudsmannens byrå.

Gärningspersonens motiv kan vara till exempel hindrande, utpressning eller spionage av en statlig aktör. Dataintrång begås av brottslingar, statliga aktörer eller även av privatpersoner.

1.5.3 Att beakta i kommunikationen

Dataintrång påverkar organisationens ledning, den dagliga verksamheten, informationsflödet och kommunikationen. Det kan bli nödvändigt att begränsa eller helt förbjuda användningen av vissa kommunikations- och ledningskanaler. Tillförlitlig informationsöverföring samt intern och eventuell extern kommunikation måste då flyttas till alternativa kanaler.

Vid ett dataintrång kan det ta tid att utreda händelsens omfattning och effekter. Organisationen måste dock kommunicera snabbt, i rätt tid, öppet och till eventuella drabbade. Ett börsbolag, det vill säga ett bolag vars värdepapper är föremål för handel, ska i sin kommunikationsplanering beakta eventuell uppkomst av insiderinformation som kan påverka

marknaden och offentliggöra denna i enlighet med gällande reglering. Det handlar om att vinna eller återvinna avgörande förtroende för organisationens verksamhet och framtid.

Kommunikationen bör förberedas utifrån det värsta scenariot, det vill säga att alla eller vissa uppgifter som organisationen innehar (kund- och personuppgifter samt uppgifter om anställda) har läckt till brottslingar.

Om personuppgifter har hamnat hos angriparen vid ett cyberangrepp är det viktigt att förstå att risken ur offrets perspektiv aldrig upphör. Risken är särskilt stor om det rör sig om känsliga uppgifter som hälsouppgifter. Brottslingar kan när som helst i framtiden offentliggöra informationen igen, till exempel för utpressning eller för att skada offrets rykte. Därför är det viktigt att komma ihåg att en informationsläcka är en kris som aldrig tar slut ur offrets perspektiv. Därför måste organisationer fästa särskild uppmärksamhet vid efterkommunikation och informationsöverföring till alla som har påverkats av situationen.

Det är avgörande att den som drabbats av en kränkning av informationssäkerheten omedelbart får lättförståelig information om vad som har inträffat, vilken risk situationen innebär för hen, samt så tydliga handlingsanvisningar som möjligt för att kunna skydda sig och vidta åtgärder snabbt. Organisationens skyldigheter vid kränkningar av informationssäkerheten beskrivs närmare i kapitel 3.1 Dataskyddsskyldigheter i denna anvisning.

Bild 4. Dataintrånget kan leda till ett dataläckage, om angriparen får tillgång till känslig information i informationssystemet.

1.6 Teknologisk utveckling förändrar hotbilden

Den teknologiska utvecklingen förändrar hotbilden snabbt. Möjligheten till ekonomisk vinning och den sänkta tröskeln för att delta i kriminell verksamhet som tekniken bidrar till lockar nya aktörer.

Bedrägerikampanjer i organisationers namn blir i framtiden allt mer sofistikerade, skräddarsydda och målinriktade. Det blir allt svårare att identifiera dem som bedrägerier. Gränsen mellan verklighet och fiktion blir allt mer suddig.

Olika AI-teknologier, -applikationer och -tjänster utvecklas snabbt och blir allt vanligare i vår vardag. Till exempel generativ AI hjälper till att hitta information i stora datamängder och skapa olika typer av innehåll. Med AI kan man skapa virtuella kopior av människor genom att kombinera röst, video, text och bilder. Sådan teknik har använts i filmer och sociala medier, såsom i Metaversum, där virtuella AI-avatarer av verkliga personer skapas.

Deepfake-teknik kombinerar olika metoder för att skapa till exempel falska videor där en person gör eller säger saker som hen aldrig gjort i verkligheten. Tekniken används redan i bedrägerier, för att svärta ner personers rykte och sprida desinformation. AI kan skapa trovärdiga virtuella kopior baserat på endast ett ljud- eller videoklipp och till och med förfalska videosamtal i realtid.

Begreppet ”deepfake” avser flera tekniker

- Dessa är till exempel ersättning av en persons ansikte i en video med ett annat, så att det ser ut som om personen gör något hen aldrig gjort.
- Dessutom går det att synkronisera läpprörelser så att personen på videon verkar säga saker hen aldrig sagt.
- Bildmanipulation kan användas för att skapa verklighetstrogna fotografier av personer, vilket kan användas i falska profiler i sociala medier.
- I ljuddeepfakes används en persons röst för att skapa innehåll till exempelvis sociala medier som får det att låta som om personen säger något hen aldrig sagt.
- Tekniken möjliggör redan imitation av en målpersons gester och ansiktsuttryck, vilket ökar trovärdigheten hos falska videor.
- Brottslingar kan också använda AI för att kombinera stulna personuppgifter från dataintrång med offentligt tillgänglig information.

Hot och risker får ofta stor publicitet. Det är ändå viktigt att komma ihåg att teknologisk utveckling, även om den medför nya hot och förändrar existerande, också erbjuder verktyg för att motverka dem. Ny teknik kan alltså både skapa och motverka risker och hot.

2 Kommunikation vid cybersituationer

Den egna organisationen kan vara ett direkt mål för ett cyberangrepp, men det kan också bli en del av en så kallad leveranskedjeangrepp. Vid ett leveranskedjeangrepp riktas angreppet inte direkt mot den egna organisationen utan mot en annan aktör, men konsekvenserna kan ändå påverka den egna organisationen, till exempel om det finns nätverks- eller systemförbindelser till den angripna parten. Känslig information som tillhör organisationen kan också hamna i brottslingars händer via ett framgångsrikt dataintrång i en annan organisations system.

I sådana situationer behövs ett smidigt och förtroendefullt informationsutbyte mellan organisationer för att säkerställa en enhetlig och snabb kommunikation.

Vanligtvis måste en organisation kommunicera om cyberangrepp eller dess konsekvenser mycket snabbt. Den egna personalen, kunderna och olika samarbetspartners förväntar sig information om det som har hänt samt tydliga handlingsanvisningar.

Vid planering och genomförande av kommunikationen måste olika målgrupper beaktas, såsom: den egna personalen, kunder, eventuella särskilda grupper som är direkt påverkade av angreppet, samarbetspartner, avtalspartners/underleverantörer, andra aktörer inom branschen, medier, intressentgrupper och beslutsfattare.

Vid planering och genomförande av kommunikationen beaktas olika målgrupper, såsom

- den egna personalen,
- kunder,
- eventuella särskilda grupper som är direkt påverkade av angreppet,
- samarbetspartner,
- avtalspartners/underleverantörer,
- andra aktörer inom branschen,
- medier,
- intressentgrupper och
- beslutsfattare.

2.1 Ledning och kommunikation vid cybersituationer

Sex nyckelprinciper för kommunikation

1. Situationen leds och kommuniceras även när inte all information är tillgänglig.
2. En tillförlitlig organisation kommunicerar själv alltid när det är möjligt.
3. I kommunikationen betonas en beskrivning av händelsen och tydliga instruktioner.
4. Långsiktigt stöd till angreppets offer.
5. Kom ihåg att internationell kommunikation kan behövas.
6. Regelbunden kommunikation bygger förtroende.

Vid cyberangrepp tillämpas samma kommunikationsprinciper som i den dagliga kommunikationen, men mängden och hastigheten ökar. Det är viktigt att kommunikationen är aktuell och tydlig. Kommunikationen måste beakta olika målgrupper, deras informationsbehov samt eventuell reglering, såsom kraven på offentliggörande av insiderinformation.

Ledning, hantering och kommunikation sker särskilt i inledningsskedet i en situation där det finns fler öppna frågor än svar. Alla frågor kan inte ens identifieras. I vissa situationer, till exempel vid ett angrepp med ett utpressningsprogram, kan de verktyg och kanaler som normalt används i vardagen – särskilt de som är avgörande för ledning, informationsöverföring och kommunikation – vara otillgängliga. Om organisationen inte har en tydlig bild av var angriparen har tagit sig in i datanätet, måste man i en sådan situation begränsa verksamheten, verktygsanvändningen och informationsflödet för att undvika ytterligare skador.

Organisationer måste även förstå att personal, offentligt synliga experter eller deras familjemedlemmar kan utsättas för riktade trakasserier på grund av det inträffade. Därför är det avgörande att organisationen har tydliga riktlinjer, praxis och stödmekanismer som inkluderar psykosocialt stöd, säkerställande av fysisk trygghet samt rättsliga skyddsåtgärder. Tydliga handlingsmodeller för att hantera trakasserier och förföljelse, i kombination med starkt stöd från ledningen, signalerar både internt och externt vilka värderingar och principer organisationen står för.

2.1.1 Situationen leds och kommuniceras även när inte all information är tillgänglig

Krisledning spelar en central roll för att hantera situationen och säkerställa verksamhetens kontinuitet. Varje organisation bör ha en krisgrupp som är sammansatt enligt organisationens behov. Gruppen bör omfatta representanter från kommunikation, juridik, personalförvaltning (HR), IT samt affärs- och operativ verksamhet. Krisgruppens sammansättning beror på organisationens storlek och struktur. Det är mycket viktigt att krisgruppen har direkt och omedelbar kontakt med den högsta ledningen. Detta säkerställer snabb beslutsfattning och effektivt samarbete under krisens gång.

Det är mycket sannolikt att den ursprungliga lägesbilden över vad som har hänt, dess konsekvenser och påverkan förändras i takt med att utredningen fortskrider. Men man kan inte vänta på slutresultatet. Det är viktigt att kommunicera åtminstone på en allmän nivå för att undvika ett informationsvakuum.

Man kan till exempel säga att situationen och dess omfattning utreds. I första hand kommunicerar man sådant som man har full visshet om. Man kan också informera om att kunskapen och förståelsen av det inträffade hela tiden fördjupas.

Undvik att uttala dig säkert om sådant du inte har full kännedom om. Om organisation har gett felaktig information måste detta rättas till omedelbart. Ledningen bör synas också offentligt.

I ledningen och kommunikationen är det viktigt att redan från början överväga hur situationen kan utvecklas, vilka oväntade saker som kan framkomma, och hur den inledande kommunikationen påverkar målgruppernas uppfattning om hur effektivt och trovärdigt situationen hanteras. Det handlar om att förutse och förbereda för framtida kommunikationsbehov och ledningsbeslut.

2.1.2 En tillförlitlig organisation kommunicerar själv alltid när det är möjligt

En utmaning i kommunikationen vid cybersituationer är också att den kriminella angriparen eller annan aktör kan ta initiativet i kommunikationen. Till exempel kan brottslingen innan organisationen ens hunnit skapa sig en helhetsbild av vad som har hänt offentliggöra sin gärning genom att skicka ett krav på lösensumma eller genom att publicera interna e-postmeddelanden, dokument eller kunders känsliga personuppgifter på nätet. Därför är det viktigt att organisationen har förmåga och beredskap att reagera snabbt även kommunikativt i snabbt föränderliga situationer.

Beredskap och övning är nyckelord i detta sammanhang. Snabb reaktionsförmåga förutsätter att roller, ansvar och kommunikationsmaterial samt innehåll för olika cybersituationer har förberetts i förväg. På så sätt undviker man att förlora dyrbar tid när det krävs snabba åtgärder, förebygger ytterligare skador samt skyddar och stöttar de drabbade.

2.1.3 I kommunikationen betonas en beskrivning av händelsen och tydliga instruktioner

Målgrupperna för kommunikationen är i huvudsak vanliga människor som inte har kännedom om detaljer inom cybersäkerhet eller tekniska termer. Därför är det viktigt att använda ett begripligt språk i kommunikationen och undvika teknisk jargong. Fokus bör ligga på en tydlig beskrivning av händelsen och dess konsekvenser samt på att ge klara handlingsanvisningar. Information bör även kunna ges på olika språk.

Kommunikationen måste planeras för att säkerställa att personalen och alla berörda parter kan bilda sig en helhetsbild av vad som inträffat, veta hur de ska agera och kunna bevaka sina rättigheter. Tydlig och regelbunden kommunikation bidrar också till att förebygga eventuella ytterligare skador.

Situationen kan väcka intresse i medierna, och därför är det viktigt att informera personalen om organisationens kommunikationsansvar under händelsen: Vem ansvarar för kommunikationen och vem eller vilka ger intervjuer eller uttalanden till medierna? Att tydligt definiera kommunikationsroller och -ansvar och att kommunicera dessa till personalen hjälper till att förhindra spridning av motstridig information och budskap.

2.1.4 Långsiktigt stöd till angreppets offer

Om känsliga personuppgifter har hamnat hos angriparen till följd av ett cyberangrepp är det viktigt att komma ihåg att informationsläckan, ur offrets perspektiv, är en kris som aldrig riktigt tar slut. Brottslingen eller brottslingarna kan när som helst i framtiden offentliggöra informationen igen, till exempel i syfte att utpressa, trakassera eller smutskasta offret. Därför måste efterkommunikation och informationsflöde till alla som berörts av händelsen prioriteras även efter att det tekniska utredningsarbetet avslutats och den operativa verksamheten återgått till det normala. I många fall kan offer för cyberbrott uppmanas att vända sig till stödorganisationer som Brottsofferjouren, som erbjuder stöd och praktiska råd vid brott.

2.1.5 Glöm inte behovet av internationell kommunikation

Om organisationen har verksamhet utanför Finland (t.ex. dotterbolag), måste kommunikationen beakta det aktuella landets reglering, skyldigheter och anvisningar. Detta gäller kommunikationen till såväl organisationens anställda som till avtalspartner och kunder. Det är viktigt att alla anställda, oavsett verksamhetsland, får tydliga, tillräckliga och aktuella instruktioner om vad som har hänt, vad situationen kan innebära för dem och hur de ska agera. Detsamma gäller även kunder, underleverantörer och övriga avtalspartner.

Eftersom informationsmiljön numera är genuint internationell och inte känner några landsgränser, bör organisationen komma ihåg att en cybersäkerhetssituation kan väcka intresse i internationella medier eller spridas brett via sociala medier. Organisationen måste därför vara beredd att kommunicera även på andra språk än finska. När man kommunicerar med utländska intressentgrupper är det ofta till hjälp att kortfattat förklara det finländska verksamhetsfältet och dess aktörer, om dessa inte är kända från förut.

2.1.6 Regelbunden kommunikation bygger förtroende

Under ett cyberangrepp och det efterföljande utredningsarbetet är det bra att redan från början ange när nästa informationsuppdatering kommer. Även om det inte finns någon ny information, är det bättre att säga det än att vara tyst, om man tänker på de drabbades perspektiv. Genom regelbunden kommunikation säkerställs att olika målgrupper vet att situationen hanteras och att de inte har glömts bort. Det skapar också tillit till att de får aktuell information om frågor som berör dem så snart sådan finns att tillgå.

Människors frågor är mycket konkreta och personliga och man vill snabbt ha information

- Vad har hänt och varför?
- Vem ligger bakom en sådan här händelse?
- Vilken information om mig har läckt?
- Varifrån och av vem får jag mer information och hur ska jag agera nu?
- Hur påverkar det här mig?
- Vilka negativa konsekvenser kan detta få för mig?
- Vem ersätter eventuella skador? Kunde jag ha gjort något för att förhindra detta?
- Vilka åtgärder har ni vidtagit med anledning av detta? Hur säkerställer ni att det inte händer igen?

Underleverantörer, kunder och andra avtalspartner behöver information

- Vad har hänt och varför?
- Vem ligger bakom en sådan här händelse?
- Vilken information har läckt?
- Varifrån och av vem får jag mer information?
- Är informationssäkerheten och verksamheten i min egen organisation också hotad?
- Har angriparen tagit sig in även i våra system?
- Hur bör min egen organisation agera nu?
- Hur påverkar händelsen vår operativa verksamhet och våra egna kunder?
- Vem ersätter eventuella skador som uppstår för vår organisation?

2.1.7 Spekulation skapar osäkerhet, rädsla och spridning av felaktig information

Att namnge och peka ut den aktör som ligger bakom ett cyberangrepp är inte enkelt. I den digitala världen kan en angripare enkelt dölja sina spår eller vilseleda genom att få det att se ut som om någon annan ligger bakom. I vissa fall kan det också vara svårt att bedöma motivet bakom angreppet. Dessa faktorer bör tas i beaktande när man kommunicerar och kommenterar det inträffade – särskilt om det finns misstankar om statligt cyberspionage.

Vid kommunikation om cyberangrepp är det rekommenderat att undvika spekulation. Spekulation bygger ofta på förhandsinformation eller antaganden som inte nödvändigtvis stämmer i den aktuella situationen. I oklara lägen, särskilt i angreppets inledningsskede, kan spekulation kring hot och risker leda till ökad osäkerhet, rädsla och spridning av felaktig eller vilseledande information (desinformation eller missinformation). Kommunikationen bör fokusera på att förmedla korrekt och aktuell information utan att försköna brister eller fel. Betydelsefulla felaktigheter ska rättas till omedelbart och organisationen bör dessutom kontinuerligt följa upp målgruppernas informationsbehov.

2.2 I kommunikationen måste olika anvisningar, begränsningar och regler beaktas

2.2.1 Statsförvaltningens kommunikation vid cyberstörningar

Vid kommunikation i olika cyberstörningar tillämpas de principer som anges i Anvisningen om intensifierad kommunikation inom statsförvaltningen[2] (Statsrådets kanslis publikationer 2019:24).

Vid störningar leder den behöriga myndigheten den operativa verksamheten och ansvarar även för kommunikationen. Varje ministerium svarar för kommunikationen som gäller den egna verksamheten och för samordningen av kommunikationen inom sitt förvaltningsområde.

I situationer som berör flera myndigheter ska den myndighet som leder verksamheten se till att andra berörda myndigheter får tillräcklig information om händelsen. I en sådan situation ansvarar de behöriga myndigheterna fortsatt för kommunikationen om den operativa verksamheten eller exempelvis förundersökningen. Den ledande myndigheten svarar också för att statsrådets lägescentral får uppdaterad information om händelserna.

Vid cyberstörningar kan ledningsansvaret för kommunikationen genom beslut av statsrådet överföras till statsrådets kansli. En sådan situation kan till exempel vara ett cyberangrepp som i stor utsträckning slår ut kritisk infrastruktur och förlamar samhällsfunktioner. Också i en sådan situation ansvarar de behöriga myndigheterna för kommunikationen om den operativa verksamheten eller exempelvis förundersökningen. Samtidigt blir det allt viktigare att myndighetskommunikationen samordnas med statsledningens kommunikation. Vid störningar är det avgörande att statsrådet och myndigheterna kan tillhandahålla aktuell och tillförlitlig information som minskar de skadliga effekterna av eventuella försök till samhällspåverkan.

Myndigheterna ska komma överens om den inbördes ansvarsfördelningen och informera om förändringar i den samt säkerställa att kommunikationen är enhetlig. Samarbetet med de viktigaste intressentgrupperna fortsätter också i störningssituationer. Samarbetsformerna fastställs redan under normala förhållanden.

[2] Anvisning om intensifierad kommunikation inom statsförvaltningen: Kommunikationen under normala förhållanden och i störningssituationer - Valto

2.2.2 Kommunernas kommunikation vid cyberstörningar

Innehållet i denna anvisning kan direkt utnyttjas för att utveckla kommunernas kommunikation vid cyberstörningar. De cyberhot som beskrivs i kapitel 2 i denna anvisning är typiska risker även i kommunernas digitala verksamhetsmiljö. Att varna för nätfiskekampanjer samt att kommunicera om eventuella driftavbrott orsakade av överbelastningsangrepp eller utpressningsprogram bör redan vara en relativt etablerad form av ”grundläggande störningskommunikation” inom kommunsektorn.

En dataintrångssituation är den mest omfattande och utmanande kommunikationssituationen som kan drabba en kommun då det gäller cyberstörningar. Den kan kräva kriskommunikation riktad till hela kommunens befolkning eller till och med till invånare i ett bredare område. Att kommunicera om ett dataintrång kräver större kommunikationsresurser än normalt och betydligt mer långsiktigt arbete. Kommunerna måste också kunna identifiera och reagera på situationer som involverar hybridpåverkan.

Även vid cyberstörningar följer kommunerna sina egna kommunikationsprinciper och rutiner. När det inträffar något utöver det vanliga ökar informationsbehovet snabbt. Kommunikationen bör då vara snabb, tydlig och långsiktig. Stora förväntningar ställs på ledarskapets och kommunikationens effektivitet, förväntningar som inte kan uppfyllas utan beredskap och övning.

En grundförutsättning för att kommunens kriskommunikation ska fungera är att den dagliga kommunikationen fungerar väl och har en nära koppling till ledningen. I specialsituationer hanteras kommunikationen genom att förstärka de processer som är välfungerande och tillförlitliga.

Ett särskilt kännetecken för kommunikation vid undantagsförhållanden i kommunsektorn är att aktörsfältet är mycket brett. Vid en störningssituation behöver kommunen sannolikt skapa en lägesbild och samarbeta med såväl statliga myndigheter, välfärdsområdet och andra kommuner som med egna koncerninterna aktörer. Dessa kontakter bör etableras i förväg och samarbetsformerna övas innan en kris inträffar.

Som en del av beredskapen för cyberstörningar bör kommunen även öva på förhandskommunikation: att informera om att kommunen förbereder sig för cyberstörningar och arbetar aktivt för att skydda sina digitala tjänster. Kommunen kan också vidareförmedla myndigheternas anvisningar och rekommendationer till invånarna om hur de kan skydda sin egen digitala verksamhet mot cyberbrott.

Ofta speglar sig alla slags samhällsstörningar även på lokal nivå. Av alla aktörer inom den offentliga sektorn är kommunen den som står närmast invånarna. Invånarna är vana vid att vända sig till kommunen för att få information, även i situationer där störningen eller krisen inte direkt gäller kommunorganisationen. Kommunen kan alltså behöva kommunicera även om störningar som inte direkt rör den egna verksamheten. Intressentgrupperna bör därför identifiera kommunens breda roll och ta hänsyn till den redan i förberedelserna och i sina planer för hantering av störningssituationer.

Kommunförbundet har år 2020 publicerat handboken Kommunikation i kriser och exceptionella situationer - handbok för kommunerna (https://www.kommunforbundet.fi/publikationer/2020/2053-kommunikation-i-kriser-och-exceptionella-situationer-handbok-kommunerna), som kan användas som stöd i kommunens planering av sin kommunikation.

2.2.3 Börsmeddelanden

Om ett företag är börsnoterat omfattas det av reglerna för börsmeddelanden.

Ett börsbolag, det vill säga ett bolag vars värdepapper är föremål för handel, måste i sin informationsgivning beakta att cyberstörningar kan ge upphov till insiderinformation vars offentliggörande regleras i marknadsmissbruksförordningen. Dessa bestämmelser gäller emittenter vars värdepapper är föremål för handel både på den reglerade marknaden vid Helsingforsbörsen och på handelsplattformen First North Finland.

Med insiderinformation avses information av specifik natur som inte har offentliggjorts, som direkt eller indirekt rör emittenten och som, om den offentliggjordes, sannolikt skulle ha en väsentlig inverkan på värdepapperets pris. Emittenten ska bedöma om informationen uppfyller kriterierna för insiderinformation.

Insiderinformation ska offentliggöras så snart som möjligt. I vissa situationer som beskrivs i regleringen kan dock en emittent på eget ansvar skjuta upp offentliggörande av insiderinformation till exempel om omedelbart offentliggörande sannolikt skulle skada legitima intressen för emittenten. Mer information om offentliggörande av insiderinformation finns på Finansinspektionens webbplats *Offentliggörande av insiderinformation och uppskjutande av offentliggörande - Insiderfrågor - www.finanssivalvonta.fi*

Utöver att följa regleringen om offentliggörande av insiderinformation ska emittenten även beakta bestämmelserna i värdepappersmarknadslagen om förbud mot att lämna osann eller vilseledande information, samt börsens regler som också innehåller anvisningar om informationsgivning.

2.2.4 Begränsningar till följd av brottsutredning

När polisen inleder en förundersökning av ett misstänkt brott kan utredningen medföra begränsningar för organisationens egen kommunikation. Kommunikationen måste planeras och genomföras så att den inte stör eller äventyrar utredningen. I samråd med förundersökningsledaren är det möjligt att säkerställa att kommunikationen inte äventyrar genomförandet av utredningen.

Polisen rekommenderar att organisationer gör en polisanmälan så tidigt som möjligt om det finns anledning att misstänka att ett brott har begåtts mot dem.

Vid cyberspionage är det utöver förundersökningen särskilt viktigt att beakta de utrikes- och säkerhetspolitiska konsekvenserna för Finland. Till exempel är det statens högsta ledning som, baserat på myndigheternas utredningar, fattar beslut om huruvida en främmande stat ska pekas ut som gärningsman i ett cyberspionagefall.

2.2.5 NIS2-direktivet och kommunikationsskyldigheter

Europeiska unionens NIS2-direktiv innehåller bestämmelser om informationssäkerhetsskyldigheter och rapportering av störningar inom olika sektorer. Direktivet ålägger särskilt kritiska sektorer att stärka cybersäkerheten genom riskhantering och rapporteringsskyldigheter. Direktivet fastställer minimiåtgärder som alla organisationer måste vidta för att hantera cybersäkerhetsrisker.

Organisationer som omfattas av NIS2-direktivets tillämpningsområde[3] är skyldiga att anmäla betydande incidenter till tillsynsmyndigheten. Betydande incidenter kan orsaka allvarliga driftstörningar eller ekonomiska förluster. Med en betydande incident avses en incident som har orsakat eller kan orsaka allvarliga driftsstörningar för tjänsterna eller betydande ekonomiska förluster för den berörda aktören, samt en incident som har påverkat eller kan påverka andra fysiska eller juridiska personer genom att orsaka betydande materiell eller immateriell skada. NIS2-direktivet

[3] Viktig information om Europeiska unionens cybersäkerhetsdirektiv (NIS2) | Cybersäkerhetscentret

förutsätter att organisationer kommunicerar tydligt, snabbt och transparent både med myndigheter och med kunder och särskilt under och efter informationssäkerhetsincidenter.

Aktören ska utan onödigt dröjsmål underrätta de mottagare av deras tjänster som kan påverkas av ett betydande cyberhot om eventuella åtgärder eller avhjälpande arrangemang som dessa mottagare kan vidta som svar på hotet.

NIS2-direktivet påverkar organisationers kommunikation särskilt vad gäller rapporteringsskyldigheter och informationsdelning

- **Rapporteringsskyldighet till myndigheter:** NIS2-direktivet ålägger organisationer att utan dröjsmål rapportera betydande informationssäkerhetsincidenter till tillsynsmyndigheterna. Den första anmälan ska göras inom 24 timmar och den uppföljande anmälan inom 72 timmar från det att den betydande incidenten upptäcktes. Detta innebär att organisationer måste vara förberedda på att snabbt samla in information om incidenten och vidarebefordra den till myndigheterna.
- **Kommunikation med kunder:** Om en incident sannolikt påverkar tillgängligheten till tjänster, ska organisationen informera sina kunder om händelsen så snart som möjligt.
- **Intern kommunikation:** Organisationer ska säkerställa att personalen får aktuell information om det inträffade samt tydliga handlingsanvisningar.
- **Slutrapport:** Organisationen ska lämna en slutrapport till myndigheterna inom en månad från det att den kompletterande anmälan lämnades in eller, om det är fråga om en långvarig incident, inom en månad från det att hanteringen av den avslutades. Rapporten ska innehålla
    - en detaljerad beskrivning av incidenten, dess allvarlighetsgrad och konsekvenser,
    - en utredning över typ av hot eller grundorsak som sannolikt orsakade incidenten,
    - en utredning över åtgärder som vidtagits och pågår för att lindra incidentens konsekvenser och
    - en utredning över eventuella gränsöverskridande konsekvenser.

2.2.6 Anmälan och kommunikation om personuppgiftsincidenter

Om ett cyberangrepp riktas mot personuppgifter, det vill säga uppgifter som direkt eller indirekt kan identifiera en person, är det fråga om en personuppgiftsincident. Då är organisationen skyldig att följa skyldigheterna i den allmänna dataskyddsförordningen (GDPR).

Den allmänna dataskyddsförordningen anger bland annat i vilka situationer organisationen ska anmäla en personuppgiftsincident till dataombudsmannens byrå och till personerna som drabbats av incidenten. Ansvar för att kommunicera om personuppgiftsincidenter vilar enligt lagstiftningen på den personuppgiftsansvarige, det vill säga den organisation som ansvarar för behandlingen av personuppgifter.

Organisationens lagstadgade anmälningsskyldigheter bestäms utifrån den risknivå som incidenten medför för de drabbade (risk för personens rättigheter och friheter).

Vid bedömningen av risknivån ska man beakta bland annat

- typen av personuppgiftsincident,
- personuppgifternas art, känslighet och omfattning,
- hur lätt personerna kan identifieras utifrån uppgifterna,
- om incidenten gäller exempelvis barn eller andra sårbara personer,
- organisationens sektor och roll samt
- hur allvarliga och sannolika konsekvenserna av dataläckaget är.

Om en personuppgiftsincident kan medföra en risk för personerna, ska dataombudsmannens byrå underrättas. Anmälan ska göras utan onödigt dröjsmål senast inom 72 timmar efter det att incidenten upptäcktes, även om alla omständigheter kring händelsen ännu inte är helt utredda. Tröskeln för att göra anmälan till dataombudsmannen kräver inte att risken är hög eller sannolik.

Om incidenten sannolikt medför en hög risk för enskilda personer, måste även de individer vars uppgifter har äventyrats underrättas. Anmälan ska ske utan onödigt dröjsmål så att personerna har möjlighet att vidta skyddsåtgärder, till exempel genom att spärra sitt kreditkort. Vid brådskande situationer som kräver snabba åtgärder ska individerna informeras så snart som möjligt.

Anmälan ska innehålla åtminstone

- en tydlig beskrivning av vad som har inträffat,
- de sannolika konsekvenserna för individen,
- de åtgärder som organisationen har vidtagit eller planerar att vidta för att mildra eventuella negativa effekter, samt
- kontaktuppgifter till organisationens dataskyddsombud eller annan person som kan ge ytterligare information.

Huvudregeln är att individerna ska informeras personligen. I vissa situationer är detta dock inte möjligt, till exempel om de berörda individerna inte kan identifieras. I sådana fall kan det vara möjligt att lämna information på annat sätt, till exempel genom offentlig delgivning. Organisationen måste dock kunna bevisa att det inte är möjligt att identifiera de berörda individerna så att de kan kontaktas direkt. Oavsett metod ska kommunikationen vara lika effektiv. Situationer där individuell information inte krävs enligt lag regleras mer i detalj i artikel 34 i dataskyddsförordningen.

Alla åtgärder som rör personuppgiftsincidenter ska dokumenteras. Mer information om organisationens skyldigheter vid personuppgiftsincidenter finns på dataombudsmannens byrås webbplats: https://tietosuoja.fi/sv/personuppgiftsincidenter.

2.3 Beredskap

Med god beredskap säkerställs att organisationen är redo och kapabel att snabbt kommunicera om ett angrepp, att spridningen av felaktig information minimeras och att alla parter får korrekt information i rätt tid. Att utarbeta kriskommunikationsplaner är obligatoriskt inom till exempel finanssektorn[4].

Frågor att beakta i beredskapsarbetet:

- Vilka är de centrala arbetsverktygen och kommunikationskanalerna i vårt arbete? Hur kan vi arbeta och kommunicera utan dem?
- Vilka typer av cyberhot kan riktas mot vår organisation? Hur svarar vi kommunikativt på dem, med beaktande av olika målgrupper och kanaler?
- Vilken information eller vilka register är kritiska för vår organisations verksamhet och vars läckage till brottsliga aktörer kan äventyra vår verksamhet eller allmänhetens förtroende för oss? Vems uppgifter finns i dessa register?
- Vilka kommunikativa åtgärder (t.ex. meddelanden och innehåll för olika situationer och målgrupper) kan vi förbereda i förväg?
- Vår organisation är verksam i flera länder, vilka är anvisningarna i respektive land för organisationer och enskilda individer vid exempelvis dataläckage eller angrepp med utpressningsprogram?
- Hur organiserar vi vår verksamhet vid olika cybersituationer? Är rollerna och ansvaret tydligt definierade?
- Vilka råd och rekommendationer kan vi ge till offer för personuppgiftsincidenter för att mildra de negativa konsekvenserna?
- Har vi kartlagt kontaktpersoner och avtalat om informationskanaler med våra viktigaste intressentgrupper och målgrupper för cybersituationer?
- Hur säkerställer vi tillförlitliga kanaler för informations- och budskapsutbyte inom organisationen?
- Hur får vi ut information om det inträffade och handlingsanvisningar till personalen i situationer där exempelvis intranätet eller e-postsystemet inte fungerar?

[4] Europaparlamentets och rådets förordning (EU) 2022/2554 om digital operativ motståndskraft för finanssektorn (DORA), artikel 14.

- Hur får vi ut information och anvisningar till våra kunder, externa samarbetspartner och intressenter i situationer där de normala externa kommunikationskanalerna helt eller delvis är ur bruk?
- Hur säkerställer vi resurser för kommunikationen och personalens ork i en långvarig krissituation?
- Hur förbereder vi oss på att vår personal kan utsättas för trakasserier eller riktad förföljelse till följd av det inträffade?
- Hur är vi förberedda på situationer där angriparens syfte är att offentligt utmana organisationen eller där alla parter inte agerar i god tro?

2.4 Kommunikation under en cyberkris

- Hur organiserar vi ett tillförlitligt informationsflöde mellan experterna som hanterar situationen och eventuella externa samarbetspartner?
- Hur får vi en aktuell lägesbild och tillgång till information för planering och genomförande av kommunikationen?
- Finns det kommunikationsrepresentation i alla grupper som behandlar och hanterar situationen?
- Vilka aktörer och organisationer bör inkluderas i kommunikationssamordningen? Vilka utanför vår egen organisation kan också beröras av just denna händelse?
- Hur kommunicerar vi tekniska frågor på ett begripligt, tidsenligt och tydligt sätt till olika målgrupper?
- Hur balanserar vi öppenhet och transparens med begränsningar på grund av exempelvis en brottsutredning?
- Hur svarar vi på olika målgruppers informationsbehov?
- Hur identifierar vi alla som drabbats av en personuppgiftsincident och hur kommunicerar vi med dem? Finns det bland offren personer vars modersmål inte är finska eller svenska?
- Hur kommunicerar vi och ger anvisningar till våra anställda och kunder i olika delar av världen, med beaktande av nationella regler och föreskrifter?
- Hur når vi och ger vägledning till offer (t.ex. kunder) som inte bor i Finland och vars modersmål inte är finska eller svenska?

- Vad är det värsta tänkbara scenariot som kan ha inträffat och som vi måste vara beredda att kommunicera om?
- Om känsliga uppgifter om våra kunder eller anställda har stulits – hur många personer kan potentiellt vara berörda? Hur långt tillbaka i tiden kan uppgifter ha läckt?
- Hur förbereder vi oss på att gärningspersonen blir aktiv?
- I vilka kanaler kommunicerar vi med olika målgrupper?
- Vilken påverkan har händelsen på vår personal, våra kunder eller samarbetspartner?
- Hur ska de agera i denna situation?

2.5 Efterkommunikation

- Hur ser vi till att informationsflödet och kommunikationen fungerar även efter incidenten? Gäller detta även resurser?
- I vilka kanaler kommunicerar vi i fortsättningen om händelsen och ger uppdateringar samt eventuella nya instruktioner?
- Hur säkerställer vi att eventuella offer fortsätter få information?
- Hur kommunicerar och agerar vi om gärningspersonen börjar sprida känsliga uppgifter om personer eller utpressa offren på nytt?
- Hur informerar vi om de åtgärder vi vidtagit för att säkerställa att en liknande incident inte ska inträffa igen?

2.6 Bedömning

- Hur bedömer våra viktigaste samarbetspartner hur väl kommunikationen lyckades?
- Hur fungerade våra interna processer för informationsflöde, ledning och kommunikation?
- Fick vi tillräcklig information för att kunna planera och genomföra kommunikationen?
- Var vår beredskap tillräcklig och ändamålsenlig?

2.7 Övningsverksamhet som en del av vardagen

En ansvarsfull organisation inkluderar övning som en del av sin kontinuitets- och beredskapsplanering. När man planerar en övning är det viktigast att klargöra vilket problem eller vilken brist som man försöker åtgärda genom övningen. Ur kommunikationsperspektiv kan det handla om exempelvis att klargöra kommunikationsrollerna tillsammans med samarbetspartner, säkerställa att lagstiftningen följs vid en kris eller till exempel garantera att kommunikationen är lämplig vid ett cyberangrepp. Efter varje övning bör lärdomar och utvecklingsbehov samlas in och uppföljning säkerställa att förbättringar genomförs.

Utifrån en riskbedömning kan man definiera lämplig mängd och innehåll för organisationens övningar. Som utgångspunkt bör kommunikationspersonalen och teamet öva åtminstone en gång per år. Man behöver inte varje år genomföra en omfattande övning, utan olika former av övningar kan växla: bordsscenarier som går igenom organisationens och tjänsteleverantörernas egna processer, interna ledningsövningar som simuleras och involverar organisationens intressenter i bredare utsträckning samt omfattande beredskapsövningar med flera olika intressentgrupper – alla dessa erbjuder olika möjligheter att utveckla organisationens kriskommunikation.

I övningsverksamheten kan man utnyttja färdigt material och övningar som tillhandahålls av den offentliga förvaltningen. Taisto-övningen, som årligen ordnas av Myndigheten för digitalisering och befolkningsdata och i första hand riktar sig till organisationer inom den offentliga sektorn, erbjuder en ledd cyberövning med låg tröskel för organisationer. Material från tidigare års övningar finns fritt tillgängliga på Taistos sidor och kan användas även i egna övningar: https://dvv.fi/sv/taisto-ovningar .

TIETO-övningen, som vartannat år ordnas av Försörjningsberedskapsorganisationens Digipooli, samlar samhällskritiska aktörer för att öva på omfattande störningar som hotar samhällets cybersäkerhet. Du kan läsa mer om TIETO-övningen på övningens webbsidor: https://teknologiateollisuus.fi/digipooli/tieto/ (på finska)

Cybersäkerhetscentrets övningstjänster vid Traficom erbjuder lättillgängligt planeringsstöd för att ordna övningar och skapa scenarier. Traficom upprätthåller också på sin webbplats en förteckning över företag som erbjuder kommersiella cybersäkerhetsövningar. Övningstjänsten nås via adressen https://www.kyberharjoitukset.fi .

3 Kriskommunikationens minneslista

3.1 Beredskap

- Bedöm riskerna: Identifiera möjliga cyberstörningssituationer och skapa mycket konkreta handlings- och kommunikationsplaner för olika situationer. Beakta resursfrågor och alternativa kommunikationskanaler.
- Ansvariga personer: Definiera vilka personer som ansvarar för kriskommunikationen, deras roller och ansvar i olika situationer. Även ersättare ska utses som en väsentlig del av beredskapen.
- Informationsflöde: Säkerställ att organisationens beredskaps- och kontinuitetsplaner beaktar att kommunikationsexperter ingår i alla grupper som leder och hanterar situationer.
- Kontaktuppgifter: Håll listan över viktiga interna och externa kontaktuppgifter uppdaterad (t.ex. organisationens ledning och experter, avtalspartner, intressenter, media och kunder). Se till att uppgifterna är tillgängliga även om de vanliga system ni använder inte är i bruk.
- Övningar: Genomför regelbundet krisövningar så att ni är redo att agera.

3.2 När krisen börjar

- Bedömning av lägesbilden: Ta reda på vad som har hänt och vilken roll och vilket ansvar organisationen har i situationen. Säkerställ att ni får aktuell information om händelsen och hur den hanteras.
- Identifiering av aktörer: Vilka organisationer och experter är involverade i att hantera och leda situationen?
- Kommunikationskanaler och verktyg: Ta reda på vilka verktyg och kanaler som står till ert förfogande. Använd vid behov reservkanaler. Kom ihåg betydelsen och möjligheterna med kommunikationssamarbete.
- Identifiering av målgrupper: Fastställ vilka målgrupper som berörs av situationen och som behöver få information och handlingsanvisningar.
- Kommunikationskanaler: Välj de kanaler som bäst når ut till era målgrupper (t.ex. sociala medier, webbplats, pressmeddelanden).
- Begränsningar i kommunikationen: Ta reda på vad och hur ni får kommunicera i situationen. Säkerställ att kommunikationen inte äventyrar polisens utredning eller orsakar ytterligare skador.

3.3 Kommunikationsprinciper

- Kom ihåg öppenhet: Var ärlig och transparent. Undvik att undanhålla information – det kan skada förtroendet och äventyra organisationens framtida verksamhet. Spekulera inte och underskatta inte det inträffade.

- Identifiera dina viktigaste målgrupper: Alla vars personuppgifter kan ha äventyrats samt den egna personalen.

- Var konsekvent: Säkerställ att alla som ansvarar för kommunikationen har ett enhetligt budskap. Detta förhindrar motstridiga uttalanden och felaktiga anvisningar. Satsa på tydlig och begriplig kommunikation. Kom också ihåg regelbunden kommunikation, efterkommunikation och behovet av eventuell internationell kommunikation.

- Lyssna och stötta: Identifiera krisens påverkan på människor och visa empati i kommunikationen.

3.4 Åtgärder under krisen

- Kommunicera regelbundet: Håll alla som berörs av situationen (möjliga offer) och andra intressenter uppdaterade om utvecklingen och ge tydliga handlingsanvisningar utifrån den aktuella lägesbilden.

- Besvara frågor: Var förberedd på att svara på frågor från media, kunder och allmänheten på ett tydligt, begripligt och lugnt sätt. Om något inte är känt, erkänn det och ange när mer information eventuellt kan vara tillgänglig – återkom enligt överenskommelse.

- Förmedla korrekt information: Säkerställ att du endast delar bekräftad och korrekt information. Underskatta inte det inträffade och spekulera inte.

- Undvik informationsvakuum: Se till att information kontinuerligt och i rätt tid är tillgänglig för olika målgrupper.

3.5 Efter krisen

- Utvärdera situationen: Gå igenom krisen tillsammans med organisationens ledning och experter. Samla in respons från organisationer, samarbetspartner och intressenter som varit involverade i hanteringen av situationen. Identifiera de områden som behöver utvecklas och de arbetsmetoder som bör förbättras inför framtiden. Omsätt lärdomarna i riktlinjer och praktiskt arbete.

- Kom ihåg behovet av efterkommunikation: Möjliga offer kan behöva information, stöd och tydliga handlingsanvisningar även efter krisens akuta fas.

Kris kommunikation i samband med cyberangrepp

1 Beredskap

Bedöm riskerna
Identifiera möjliga cyberstörningssituationer och skapa mycket konkreta handlings- och kommunikationsplaner för olika situationer. Beakta resursfrågor och alternativa kommunikationskanaler.

Ansvariga personer
Definiera vilka personer som ansvarar för kriskommunikationen, deras roller och ansvar i olika situationer. Även ersättare ska utses som en väsentlig del av beredskapen.

Informationsflöde
Säkerställ att organisationens beredskaps- och kontinuitetsplaner beaktar att kommunikationsexperter ingår i alla grupper som leder och hanterar situationer.

Kontaktuppgifter
Håll listan över viktiga interna och externa kontaktuppgifter uppdaterad (t.ex. organisationens ledning och experter, avtalspartner, intressenter, media och kunder). Se till att uppgifterna är tillgängliga även om de vanliga system ni använder inte är i bruk.

Övningar
Genomför regelbundet krisövningar så att ni är redo att agera.

2 När krisen börjar

Bedömning av lägesbilden
Ta reda på vad som har hänt och vilken roll och vilket ansvar organisationen har i situationen. Säkerställ att ni får aktuell information om händelsen och hur den hanteras.

Identifiering av aktörer
Vilka organisationer och experter är involverade i att hantera och leda situationen?

Kommunikationskanaler och verktyg
Ta reda på vilka verktyg och kanaler som står till ert förfogande. Använd vid behov reservkanaler. Kom ihåg betydelsen och möjligheterna med kommunikationssamarbete.

Identifiering av målgrupper
Fastställ vilka målgrupper som berörs av situationen och som behöver få information och handlingsanvisningar.

Kommunikationskanaler
Välj de kanaler som bäst når ut till era målgrupper (t.ex. sociala medier, webbplats, pressmeddelanden).

Begränsningar i kommunikationen
Ta reda på vad och hur ni får kommunicera i situationen. Säkerställ att kommunikationen inte äventyrar polisens utredning eller orsakar ytterligare skador.

3 Kommuni-kations-principer

Kom ihåg öppenhet
Var ärlig och transparent. Undvik att undanhålla information – det kan skada förtroendet och äventyra organisationens framtida verksamhet. Spekulera inte och underskatta inte det inträffade.

Identifiera dina viktigaste målgrupper
Alla vars personuppgifter kan ha äventyrats samt den egna personalen.

Var konsekvent
Säkerställ att alla som ansvarar för kommunikationen har ett enhetligt budskap. Detta förhindrar motstridiga uttalanden och felaktiga anvisningar. Satsa på tydlig och begriplig kommunikation. Kom också ihåg regelbunden kommunikation, efterkommunikation och behovet av eventuell internationell kommunikation.

Lyssna och stötta
Identifiera krisens påverkan på människor och visa empati i kommunikationen.

4 Åtgärder under krisen

Kommunicera regelbundet
Håll alla som berörs av situationen (möjliga offer) och andra intressenter uppdaterade om utvecklingen och ge tydliga handlingsanvisningar utifrån den aktuella lägesbilden.

Förmedla korrekt information
Säkerställ att du endast delar bekräftad och korrekt information. Underskatta inte det inträffade och spekulera inte.

Besvara frågor
Var förberedd på att svara på frågor från media, kunder och allmänheten på ett tydligt, begripligt och lugnt sätt. Om något inte är känt, erkänn det och ange när mer information eventuellt kan vara tillgänglig – återkom enligt överenskommelse.

Undvik informationsvakuum
Se till att information kontinuerligt och i rätt tid är tillgänglig för olika målgrupper.

5 Efter krisen

Utvärdera situationen
Gå igenom krisen tillsammans med organisationens ledning och experter. Samla in respons från organisationer, samarbetspartner och intressenter som varit involverade i hanteringen av situationen. Identifiera de områden som behöver utvecklas och de arbetsmetoder som bör förbättras inför framtiden. Omsätt lärdomarna i riktlinjer och praktiskt arbete.

Kom ihåg behovet av efterkommunikation
Möjliga offer kan behöva information, stöd och tydliga handlingsanvisningar även efter krisens akuta fas.

4 Ytterligare information

Myndigheternas guide för offer för dataintrång och informationsläckor:
https://www.suomi.fi/guider/informationslacka

Anvisning om intensifierad kommunikation inom statsförvaltningen: Kommunikationen under normala förhållanden och i störningssituationer. Statsrådets kanslis publikationer 2019:24
https://julkaisut.valtioneuvosto.fi/handle/10024/161975

Att känna igen informationspåverkan, Cybersäkerhetscentret vid Traficom
https://www.kyberturvallisuuskeskus.fi/sv/aktuellt/tips-om-hur-man-kanner-igen-informationspaverkan-var-vaksam-och-agera-ansvarsfullt

Att möta informationspåverkan - handbok för kommunikatörer, Statsrådets kanslis publikationer 2019:13
Att möta informationspåverkan: Handbok för kommunikatörer - Valto

Dataombudsmannens byrås anvisningar till organisationer vid personuppgiftsincidenter: https://tietosuoja.fi/sv/personuppgiftsincidenter

Cybersäkerhetscentrets anvisningar och guider för organisationer och företag:
Informationssäkerhetsanvisningar till företag | Cybersäkerhetscentret

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

traficom.fi

ISBN 978-952-311-973-4
ISSN 2669-8757 (webbpublikation)

TRAFICOM
Transport- och kommunikationsverket