TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret

Anvisning – Leveranskedjeangrepp

Traficoms forskningsrapporter och utredningar
21/2022

Innehållsförteckning

1 Inledning

1.1 Syftet med anvisningen

Denna anvisning har utarbetats av Cybersäkerhetscentret vid Transport- och kommunikationsverket Traficom och syftar till att ge organisationer råd i situationer, där man misstänker ett leveranskedjeangrepp. Fokus för anvisningen ligger på att behandla särdragen för denna typ av informationssäkerhetsincident. För att lösa situationen i sin helhet är det bra om organisationen upprätthåller och följer den incidenthanteringsplan som den upprättat för informationssäkerhetsincidenter (eng. Incident Response Plan).

Denna anvisning ger övergripande vägledning för hur man ska agera vid informationssäkerhetsincidenter och hur man kan återhämta sig från dem. Det rekommenderas att organisationen upprättar en egen separat guide, som på en mer detaljerad nivå beaktar organisationens tekniska och operativa miljö. Projektet har finansierats av Försörjningsberedskapscentralen.

1.2 Vad är ett leveranskedjeangrepp?

Vid ett leveranskedjeangrepp gör någon intrång i en organisations informationssystem via de nätverk, tjänster, produkter eller projekt med öppen källkod som den använder. I angreppet utnyttjas organisationens förtroende för sina leverantörer. Angreppet kan gå via samarbetspartner, tjänsteleverantörer, programvaror eller enheter. Angriparen tar sig in i leverantörens system och infekterar en del av leveranskedjan med en skadlig kod, varefter den sprider sig via produktens normala distributionskanal till samarbets- och kundorganisationer.

Syftet med leveranskedjeangrepp är att få fotfäste någonstans i leveranskedjan i olika organisationer. När fotfästet säkerställts kan det användas för olika typer av fortsatta angrepp, till exempel dataintrång och angrepp med utpressningsprogram.

Det är viktigt att upptäcka och hantera leveranskedjeangrepp, eftersom de har stor betydelse för organisationens anseende och förtroende deras nätverk. Vid leveranskedjeangrepp är både leverantören och kunden offer. För att hantera situationen krävs ofta öppenhet och samarbete mellan parterna.

2 Beredskap

Att förbereda sig för incidenter är ett bra sätt att minska deras allvarlighetsgrad samt möjliggöra snabb återhämtning och en fortsättning på affärsverksamheten. Organisationen kan bedöma sin beredskap genom att använda till exempel Cybersäkerhetscentrets Cybermätare[1]. En i förväg upprättad incidenthanteringsplan ger ett bra utgångsläge för hur man ska agera när en incident inträffar. Organisationen ska även säkerställa att olika åtgärder, till exempel att låsa användarkoder, blockera servrar och enheter från nätverket samt begränsa nättrafiken till skadliga IP-adresser eller domännamn, är tekniskt möjliga och att personalen även har kompetens för att genomföra dem.

Det är viktigt att samla in, sammanställa och övervaka loggdata för att kunna upptäcka incidenter i tid. Loggdata gör det även möjligt att utreda incidenter grundligt och på så sätt göra rensningen och återställandet av miljön snabbare. Cybersäkerhetscentret har utarbetat anvisningar för hur man samlar in och använder loggdata.[2] Beroende på vilka system en organisation använder, krävs vanligtvis dessutom lösningar på nätverks- och systemnivå för omfattande monitorering.

2.1 Administrativa åtgärder

- Upprätta en incidenthanteringsplan för din organisation för användning i händelse av ett leveranskedjeangrepp.
- Utbilda personalen i hur den ska agera medan en sådan incident som beskrivs i denna anvisning råder.
- Ta i förväg reda på hur du kan anmäla en informationssäkerhetsincident till Cybersäkerhetscentret.[3] Följ Cybersäkerhetscentrets aktuella meddelanden.[4]
- Gå igenom olika angreppsscenarier tillsammans med ledningen och kom överens om praktiska åtgärder samt ledningsansvar och -befogenheter vid informationssäkerhetsincidenter.
- Öva på[5] och utveckla incidenthanteringsplanen regelbundet med hjälp av diskussionsbaserade övningar (eng. Tabletop Exercise) , där de ansvariga personerna och intressenterna övar på processen för hantering av informationssäkerhetsincidenter i ett fiktivt scenario.
- Inför processer för kontinuerlig hantering av sårbarheter och uppdateringar.
- Identifiera de komponenter som är kritiska för affärsverksamheten samt skapa och upprätta en förteckning över de objekt som ska skyddas.
    - För en komponentlista över de mest kritiska systemen.
- För en lista över de licenser och programvaror som organisationen använder samt deras versioner.
    - Följ deras uppdateringsscheman och sårbarheterna i dem.
- Definiera noggrant vilka behörigheter som behövs för användarna och de tekniska funktionerna.
- Utvärdera läget för leverantörernas cybersäkerhet. När du säkerställer att alla leverantörer ger en komplett beskrivning av sina säkerhetsåtgärder får du en uppfattning om hur säkra

[1] https://www.kyberturvallisuuskeskus.fi/sv/vara-tjanster/lagesbild-och-natverksledarskap/cybermataren
[2] https://www.kyberturvallisuuskeskus.fi/sv/aktuellt/anvisningar-och-guider/sa-har-samlar-du-och-anvander-loggdata
[3] https://www.kyberturvallisuuskeskus.fi/sv/anmal
[4] https://www.kyberturvallisuuskeskus.fi/sv/ajankohtaiset
[5] https://www.kyberturvallisuuskeskus.fi/sv/vara-tjanster/ovningar

deras produkter är. Du kan även be en expert på cybersäkerhet att undersöka de uppgifter som leverantörerna uppgett för att se om säkerhetslösningarna är lämpliga och tillräckliga.

- Överväg att inrätta ett säkerhetsoperationscenter eller att köpa en motsvarande tjänst. Syftet med en sådan säkerhetstjänst är att övervaka ditt företags nättrafik och informationssäkerhetsincidenter i systemen.

2.2 Tekniska åtgärder

- Säkerhetskopiera dina kritiska system regelbundet och automatiskt enligt 3-2-1-regeln. Förvara med andra ord minst tre kopior i två olika format, och en av kopiorna ska vara helt bortkopplad från nätverket.
- Testa regelbundet att säkerhetskopiorna fungerar och öva på att återställa säkerhetskopiorna åtminstone för de kritiska systemen.
- Tillämpa nätverkssegmentering, datakryptering och åtkomstbegränsning för att säkerställa att ditt företags angreppsyta är så liten som möjligt.
- Skydda samarbetspartnernas förbindelser med hjälp av starka krypteringsinställningar och inför flerfaktorsautentisering.
- Sträva efter att upptäcka angrepp så tidigt som möjligt med hjälp av olika centraliserade monitoreringslösningar, vars funktion även testas regelbundet.
- Installera programvaror som skyddar mot skadliga program på enheterna och med hjälp av vilka man kan begränsa körningen av programmen, undersöka misstänkta informationssäkerhetsincidenter och vid behov blockera en dator från nätverket.
- Inför mekanismer för filtrering av e-postmeddelanden med skadligt innehåll samt skräppost och icke önskvärd nättrafik.
- En centraliserad logghantering ska tas i bruk för att göra det möjligt att effektivt upptäcka och undersöka cyberrisker.

3 Upptäcka en informationssäkerhetsincident

Det kan vara utmanande att upptäcka en informationssäkerhetsincident som genomförts via en leveranskedja, eftersom angriparen utnyttjar organisationens förtroende för sina samarbetspartner. Ofta görs intrånget genom att man använder sig av samarbetspartnernas förbindelser eller infekterar applikationen som de tillhandahåller. I sådana fall gör angriparen inte ännu när intrånget sker någonting som kan tolkas som misstänkt eller skadligt.

Ett angrepp kan upptäckas på till exempel följande sätt:

- En samarbetspartner meddelar att den fallit offer för ett cyberangrepp.
- Med hjälp av samarbetspartnerns användarkoder försöker någon logga in i tjänster som den normalt inte skulle logga in i.
- En informationssäkerhetsprodukt eller en tjänsteleverantör avger ett larm, som vanligtvis orsakas av en pålitlig applikation.
- Organisationen får ett meddelande om ett angrepp utifrån organisationen, till exempel via sociala medier, en kund, en samarbetspartner eller en myndighet.

Anmäl informationssäkerhetsincidenten till Cybersäkerhetscentret.[6] Vi ger er konfidentiellt och kostnadsfritt råd för hur ni begränsar skadorna, analyserar incidenten och vidtar återställande åtgärder. Samtidigt stöder ni den nationella lägesbilden av informationssäkerheten och gör det möjligt för oss att varna och hjälpa andra eventuella offer.

Läs Cybersäkerhetscentrets anvisning för hur man upptäcker dataintrång (på finska).[7]

[6] https://www.kyberturvallisuuskeskus.fi/sv/anmal
[7] https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/opas-tietomurtojen-havaitsemiseen

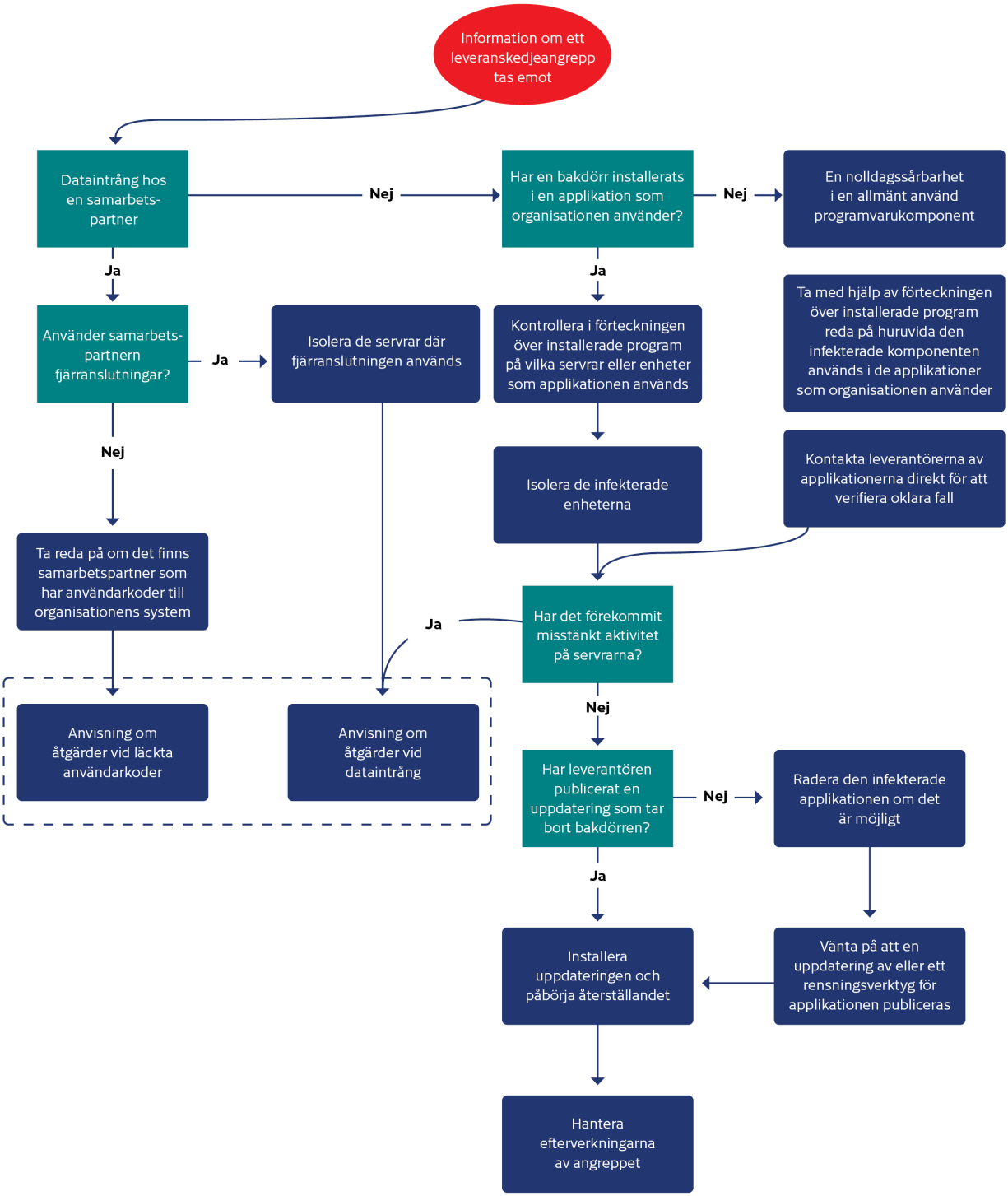
4 Anvisningar

Använd nedanstående checklista på åtgärder som hjälp när du misstänker att du fallit offer för ett leveranskedjeangrepp. Checklistan hjälper organisationen att prioritera och dela in verksamheten vid utredningen av en informationssäkerhetsincident.

4.1 Arbetsflödet vid utredning av en informationssäkerhetsincident

Nedanstående flödesplan beskriver de åtgärder som ska tillämpas för att en incident ska kunna utredas i rätt ordning. Flödesplanen stöder användningen av checklistan. Under utredningen är det även ytterst viktigt att föra en noggrann händelselogg över de åtgärder som vidtagits. Av loggen ska framgå vilken åtgärd som genomförts, tidsstämpeln för den och vem som utfört åtgärden.

Det är även skäl att omsorgsfullt dokumentera eventuellt bevismaterial. Det bör antecknas vem som samlat in materialet, vad materialet består av samt var och när det har samlats in. En omsorgsfullt upprättad händelselogg underlättar avsevärt utredningen samt samarbetet med polisen och datasäkerhetsforskarna.


Information om ett leveranskedjeangrepp tas emot
Dataintrång hos en samarbets-partner
Nej
Har en bakdörr installerats i en applikation som organisationen använder?
Nej
En nolldagssårbarhet i en allmänt använd programvarukomponent
Ja
Ja
Använder samarbets-partnern fjärranslutningar?
Ja
Isolera de servrar där fjärranslutningen används
Kontrollera i förteckningen över installerade program på vilka servrar eller enheter som applikationen används
Ta med hjälp av förteckningen över installerade program reda på huruvida den infekterade komponenten används i de applikationer som organisationen använder
Nej
Isolera de infekterade enheterna
Kontakta leverantörerna av applikationerna direkt för att verifiera oklara fall
Ta reda på om det finns samarbetspartner som har användarkoder till organisationens system
Ja
Har det förekommit misstänkt aktivitet på servrarna?
Anvisning om åtgärder vid läckta användarkoder
Anvisning om åtgärder vid dataintrång
Nej
Har leverantören publicerat en uppdatering som tar bort bakdörren?
Nej
Radera den infekterade applikationen om det är möjligt
Ja
Installera uppdateringen och påbörja återställandet
Vänta på att en uppdatering av eller ett rensningsverktyg för applikationen publiceras
Hantera efterverkningarna av angreppet

4.2 Omedelbara åtgärder

Stegets mål	Det är viktigt att åtgärderna är både exakta och snabba. Målet med de omedelbara åtgärderna är att skydda kritiska uppgifter i miljön, stoppa spridningen av den skadliga programvaran, hindra angriparna från att få fotfäste i nätverket och förbereda inledningen av återhämtningsprocessen.

Steg	Syfte	Åtgärder
Isolera den infekterade enheten	Genom att isolera den infekterade enheten från de övriga datanäten försöker man hindra angreppet från att sprida sig samt skydda informationen i systemet.	Blockera enheterna genom att använda dig av funktionerna i den centraliserade övervakningen av enheterna. Dra vid behov ur enheternas nätverkskablar. Isoleringen måste även hindra enhetens tillgång till internet, så att angriparens möjligheter att stjäla information från servern stoppas.
Ta reda på vilken förbindelse eller komponent som använts vid angreppet	Vid ett leveranskedjeangrepp kan många olika slags förbindelser användas, till exempel dataöverförings-, programuppdaterings-, system- eller serviceförbindelser. Angreppen kan även genomföras genom att utnyttja programvaror eller deras komponenter.	Ta reda på om angreppet har genomförts • via en samarbetspartners fjärranslutning eller med hjälp av läckta användarkoder, eller • med hjälp av en bakdörr som installerats i en applikation som din organisation använder. Kontrollera om programmen och systemen på den infekterade enheten är uppdaterade. Följ även Cybersäkerhetscentrets meddelanden, eftersom angreppet kan ha utförts med hjälp av en ny nolldagssårbarhet.
Ta reda på vilka servrar och arbetsstationer som kan ha infekterats vid angreppet	Man måste snabbt kunna identifiera alla servrar och enheter som använder den förbindelse eller komponent som utnyttjats i angreppet, så att samtliga enheter som eventuellt har infekterats kan isoleras.	Ta hjälp av en lista över din IT-egendom och de program som installerats för att snabbt få en uppfattning om var den infekterade applikationen eller komponenten används. Om det är fråga om en förbindelse för fjärradministration eller någon annan integration, kontrollera i dokumentationen var dessa används och varifrån man kommer åt dem. Om det är fråga om till exempel ett infekterat bibliotek som används i flera olika system, kontrollera med hjälp av en lista över installerade program vilka applikationer som används och ta reda på om den aktuella komponenten används i dem. Detta kan kräva att organisationen direkt kontaktar leverantören av applikationen för att man ska få klarhet i saken. Om någon av åtgärderna inte lyckas utan IT-tjänsteleverantörens hjälp, gå till följande punkt i anvisningen.

Kontakta din IT-tjänsteleverantör	Ofta har en del av organisationers IT-infrastruktur utkontrakterats till en tjänsteleverantör. En del åtgärder för att begränsa incidenten kan kräva tjänsteleverantörens hjälp.	Ta senast i detta skede reda på vilka delar av din organisations IT-infrastruktur som har utkontrakterats till tjänsteleverantörer. Kontakta tjänsteleverantörens kontaktperson vid krissituationer. Du kan bli tvungen att be din tjänsteleverantör att bland annat koppla bort dina servrar från nätverken, återställa dem eller skicka deras loggar. IT-tjänsteleverantörer har ofta kunnig personal, som kan vara till stor hjälp när en incident ska lösas.
Informera de samarbetspartner och intressenter som kan påverkas om informationssäkerhetsincidenten	Incidenten kan leda till risker eller problem med tillgången till tjänster för samarbetspartner, kunder och tjänsteleverantörer. Även partnernas cybersäkerhet kan äventyras till följd av ett angrepp mot leveranskedjan.	Informera intressenternas kontaktpersoner vid krissituationer om incidenten om du tror att den kan påverka tillgången till deras tjänster. Om det funnits anslutningar från servern till andra organisationer ska även dessa informeras, så att de kan göra de koder, nycklar eller certifikat som använts på den infekterade servern ogiltiga. Det är också viktigt att de kontrollerar integriteten av deras egna data. Informera vid behov även övriga organisationer i leveranskedjan, till exempel leverantörer, om incidenten.
Bedöm om du behöver utomstående hjälp för att hantera informationssäkerhetsincidenten	Organisationen kan behöva hjälp med att organisera åtgärder, hantera incidenten eller utföra tekniska åtgärder. Om det inte finns tillräcklig kompetens internt eller direkt hos IT-tjänsteleverantörerna ska man överväga att anlita hjälp utifrån.	De tekniska åtgärderna vid hanteringen av en incident kan kräva extern kompetens. Sådana åtgärder kan vara till exempel insamling av identifieringsuppgifter och utredning av hotet utifrån dem. Den externa hjälpen kan även hjälpa till att kontrollera huruvida angriparen har kommit över data som är viktig för affärsverksamheten och i så fall vilka data. Cybersäkerhetscentret kan hjälpa organisationer med i synnerhet de första insatserna och genom att erbjuda tilläggsinformation om liknande fall i Finland och internationellt. Bakom länkarna i källförteckningen hittar du finländska tjänsteleverantörer.[8]
Anmäl informationssäkerhetsincidenten till dataombudsmannens byrå	Om det är möjligt att personuppgifter har hamnat i händerna på angriparen i samband med dataintrånget ska incidenten anmälas till dataombudsmannens byrå utan oskäligt dröjsmål och i mån av möjlighet inom 72 timmar från det att organisationen har fått kännedom om informationssäkerhetsincidenten.	Gör omedelbart en preliminär anmälan om informationssäkerhetsincidenten, eftersom anmälan kan kompletteras senare. Den personuppgiftsansvarige måste bedöma hur stor risk personuppgiftsincidenten orsakar

[8] https://dfir.fi/

https://www.fisc.fi/fi

https://www.hansel.fi/sv/upphandlingar/tiedonhallinnan-ja-digiturvallisuuden-asiantuntija/

		för de personer som utsatts för den. Risknivån fastställer de åtgärder som den personuppgiftsansvarige senare måste vidta. Dokumentera alla personuppgiftsincidenter och deras konsekvenser samt vilka korrigerande åtgärder som genomförts. Beträffande en informationssäkerhetsincident i ett informationssystem omfattar dokumenteringsskyldigheten även loggdata från tidpunkten för incidenten. Dataombudsmannen kan begära logguppgifter för behandlingen av anmälan om informationssäkerhetsincidenten.
Rapportera informationssäkerhetsincidenten även till andra myndigheter	Rapportera incidenten till myndigheterna. Organisationen kan enligt författningar eller villkoren i cyberförsäkringen vara skyldig att anmäla incidenten.	Gör en brottsanmälan om händelsen till polisen.[9] Anmäl händelsen även till Cybersäkerhetscentret[10] för att upprätthålla lägesbilden och få hjälp. Aktörer och tjänsteleverantörer, som är kritiska med tanke på försörjningsberedskapen och som omfattas av EU:s direktiv om säkerhet i nätverks- och informationssystem (s.k. NIS-direktivet), ska anmäla informationssäkerhetsincidenter i nätverks- och informationssystem till myndigheterna[11].

[9] https://poliisi.fi/sv/gor-en-brottsanmalan

[10] https://www.kyberturvallisuuskeskus.fi/sv/anmal

[11] https://www.kyberturvallisuuskeskus.fi/sv/vara-tjanster/rapportera-en-it-sakerhetsincident-nis-skyldighet

4.3 Utredning av en informationssäkerhetsincident

Stegets mål	Målet med utredningen av incidenten är att ta reda på angreppets omfattning och effekt i organisationen. Genom en noggrann utredning säkerställs att skadliga programvaror och eventuella bakdörrar har avlägsnats ur miljön.

Steg	Syfte	Åtgärder
Känn igen tecken på skadlig aktivitet och samla in identifieringsuppgifter	Identifieringsuppgifter samlas in för att man ska kunna kartlägga i hur stor utsträckning enheterna har infekterats och på vilket sätt stulna behörigheter har utnyttjats. Efter att ha fått fotfäste kan angriparen använda olika angreppsmetoder. Därför ska identifieringsuppgifter samlas in i stor omfattning och tecken på att de använts undersökas noggrant, så att miljön kan rensas på ett tillförlitligt sätt. Återhämtningen kan börja först när angriparen har körts bort från samtliga miljöer.	Samla in följande identifieringsuppgifter: • När loggade man in på servern? • Från vilken IP-adress gjordes inloggningen? • Vilken tid kördes ett visst kommando på servern? • Vad fick kommandot ifråga till stånd på servern? Den skadliga programvaran kommunicerar ofta med angriparens kommandoserver. Genom att kontrollera de infekterade enheternas nättrafik eller undersöka domännamnen (DNS-loggarna) kan du identifiera den käll-IP-adress eller det domännamn som angriparen använder. Du kan ta tillvara identifierarna för de skadliga filerna (MD5/SHA256) och med hjälp av dem identifiera dem även på andra enheter. Utifrån identifieringshändelser som riktats mot de infekterade enheterna och de åtgärder som utförts med användarkonton i anknytning till dessa kan du fastställa vilka koder som använts för att sprida den skadliga programvaran. Den centraliserade övervakningen av enheterna inkluderar ofta funktioner för att samla in och använda ovannämnda identifieringsuppgifter. I annat fall ska åtgärderna utföras manuellt med hjälp av en centraliserad loggserver. Om inte heller detta alternativ är möjligt kan du undersöka de enskilda servrarnas och enheternas loggar.
Använd identifieringsuppgifterna för att identifiera alla infekterade system	Med hjälp av de insamlade identifieringsuppgifterna kan man ta reda på i hur stor omfattning angriparen har tagit sig in i organisationen. Genom att samla in identifieringsuppgifter och söka dem i målsystemen kan man verifiera att alla infekterade enheter och koder hittas och åtgärdas.	Med hjälp av identifieringsuppgifterna kan du söka infekterade enheter, till exempel genom att använda funktionerna i den centraliserade övervakningen av enheterna, vilka ofta erbjuder en direkt möjlighet att med olika identifikationskoder söka händelser på enheterna. Om din organisation även har en centraliserad logghantering kan du med hjälp av den effektivt söka händelser i flera olika datorer samtidigt på basis av identifikationskoderna. Om ingen av de ovanstående lösningarna är tillgängliga ska identifikationskoderna sökas separat på varje dator. För det kan du dock använda olika lösningar för fjärradministration, som ofta gör det möjligt att till exempel köra PowerShell-

		kommandon på flera servrar samtidigt. Det finns en risk att angriparen, efter att ha tagit sig in i en enhet, har kopplat bort insamlingen av loggar, vilket innebär att det inte finns några spår efter hans eller hennes aktivitet. Därför ska du undersöka identifieringsuppgifterna som samlats in från alla de olika källorna och med hjälp av dem försöka skapa dig en helhetsbild av angriparens aktivitet.
Ta reda på vilka anslutningar som använts på servern	Ofta har servrar anslutningar till andra system. Sådana kan vara till exempel databasanslutningar eller olika API-förfrågningar och -nycklar. För att kartlägga hur allvarlig situationen är ska man så fort som möjligt kontrollera huruvida angriparen har tagit sig in även i dessa system. Ta så fort som möjligt reda på huruvida angriparen har tagit sig in även i dessa kombinerade system genom att kontrollera deras loggar. På så sätt får du en helhetsbild av incidentens omfattning.	Om servern har anslutningar till andra system, ta reda på huruvida intrång har gjorts även i dessa genom att granska de kombinerade systemens loggar. Det kan vara fråga om att kontrollera bland annat hur stora databassökningarna som gjorts har varit eller hur stort antalet anrop till gränssnittet har varit under den tid som angriparen har befunnit sig på servern. Ändra koderna till de kombinerade tjänsterna, till exempel den databaskod som användes på den infekterade servern, API-nycklarna samt de certifikat som använts för förbindelserna.
Ta reda på om kritiska uppgifter har äventyrats	Som en del av utredningen ska man ta reda på huruvida angriparna har kommit över viktiga uppgifter om organisationen eller eventuellt personuppgifter för kunder eller anställda.	Ta reda på huruvida de koder, certifikat eller nycklar som använts i förbindelserna även använts för att logga in från något annat ställe än servern, där de är avsedda att användas. Ta reda på huruvida angriparna har kommit över och stulit uppgifter. Genom att granska databasens eller gränssnittets loggar kan du utifrån de sökningar som gjorts eller belastningsgraden avgöra huruvida angriparen har försökt ladda ner uppgifter. Kontrollera nätenheternas loggar för avvikelser i den infekterade serverns trafik. Exceptionellt tung trafik kan vara ett tecken på till exempel att angriparen har stulit information. Observera att angriparen, förutom att ha förstört och stulit uppgifter, även kan ha ändrat dem. Han eller hon kan även ha tagit mycket små mängder data, såsom användarkoder.
Spara alla tillgängliga loggfiler och övriga bevis på en hårddisk som är isolerad från nätverket för senare undersökning	Syftet med att samla in och spara bevis är att säkerställa en högklassig utredning av incidenten i efterhand, så att grundorsakerna till den kan klarläggas. Bevisen kan behövas i samband med en brottsutredning och för rättegångsförhandlingar. Om organisationen har en cyberförsäkring kan även försäkringsbolaget	Spara de loggfiler som innehåller viktig information med tanke på undersökningen av incidenten på en hårddisk som är isolerad från nätverket. Samla även in eventuella skadliga e-postmeddelanden och övriga meddelanden. Sträva efter att förvara bevisen, såsom kompletta skivavbilder och minnesprover, så enhetliga som

	kräva närmare uppgifter om incidenten samt bevis för en utredning.	möjligt. Använd en hashfunktion för att säkerställa deras integritet. Försök ta prover av de skadliga programvarorna och spara dem. Särskild försiktighet ska iakttas vid hanteringen. En säker förvaring kräver ofta yrkeskompetens. Skicka proverna till Cybersäkerhetscentret.[12]

[12] https://www.kyberturvallisuuskeskus.fi/sv/aktuellt/formedla-e-post-och-prov-till-cybersakerhetscentret

4.4 Återställande

Stegets mål	Återställandet inleds i de system som är mest kritiska för affärsverksamheten. Organisationen ska försöka återställa affärsverksamheten till det normala så snabbt som möjligt, men först när det kan göras på ett säkert sätt.

Steg	Syfte	Åtgärder
Aktivera förbindelserna på nytt och starta applikationerna	Man försöker återställa funktionen hos de av samarbetspartnernas fjärrförbindelser eller program som behövs i affärsfunktionerna.	Se innan förbindelserna aktiveras till att de är säkra och att samarbetspartnern även har lyckats rensa sina egna system och användarkoder. Säkerställ innan programmen aktiveras att nödvändiga korrigerande uppdateringar har installerats. Om ingen korrigerande uppdatering är tillgänglig, ta inte programmet i bruk och överväg att ta det helt ur bruk.
Återställ infekterade system från säkerhetskopior	Man strävar efter att återställa systemen och återgå till normal verksamhet. Systemen återställs på ett så säkert sätt som möjligt, så att angriparen inte kan ta sig tillbaka in i systemen.	Återställ systemen från säkerhetskopiorna. Tänk på att tidigare dagsspecifika (inkrementella) säkerhetskopior redan kan vara infekterade. När du återställer gamla säkerhetskopior ska du tänka på att säkerhetskopiorna kan innehålla sårbarheter, som angriparen kan ha utnyttjat under incidenten. Sträva efter att återställa systemen utan nätförbindelser samt uppdatera operativsystemet och dess applikationer innan du ansluter dem till nätet för att undvika riskerna i fråga. Om ingen lämplig säkerhetskopia finns tillgänglig, installera operativsystemet och dess applikationer på nytt. Beakta även de riskfaktorer som nämns i föregående kapitel. Försök inte rensa ett infekterat system med automatiska verktyg eller antivirusprogram, eftersom automatiska skannrar inte nödvändigtvis kan rensa systemet fullständigt. Kontrollera systemen med verktyg för bekämpning av skadliga program innan de på nytt ansluts till nätet.
Återställ infekterade användarkoder och verifiera säkerheten för koderna för systemadministratörer	Se till att inloggningsuppgifterna för samtliga infekterade användarkoder ändras, så att angriparen inte längre har tillträde till organisationens system med hjälp av koderna. Inloggningskraven för användarna skärps i mån av möjlighet.	Ändra lösenordet för de infekterade användarkoderna och återinför koderna. Ändra för säkerhets skull lösenorden för administratörskoderna och servicekoderna, utifall att angriparen skulle ha kommit över en del av dem. Informera användarna om de nya lösenorden antingen muntligt, per sms eller per telefon, men använd inte e-post eller de snabbmeddelanden som organisationen använder, eftersom angriparen fortfarande kan ha tillträde till dem. Överväg att införa tvåfaktorsautentisering för administratörskoderna och de koder som utnyttjades under angreppet. Övervaka även de koder som användes vid angreppet noggrannare efter att de återställts, för

		den händelse att angriparen på nytt kommer över dem. Om det förblir oklart hur angriparen kunde komma över vissa koder, överväg att förstöra dem och skapa helt nya koder. På så sätt försäkrar du dig om att angriparen inte kommer över koderna på nytt på samma för dig okända sätt.

5 Efterverkningar av informationssäkerhetsincidenten

När krisen är över och affärsfunktionerna normaliserat sig är det viktigt att börja hantera efterverkningarna av incidenten och lära sig av det inträffade för framtiden. Samtidigt är det skäl att uppdatera krishanteringsplanerna utifrån de observationer som gjorts. Det är möjligt att organisationen på nytt faller offer för en liknande incident om grundorsakerna till det inträffade inte kommer fram och man inte tar lärdom av händelsen.

Vid hanteringen av efterverkningarna (eng. Post-Incident Review) granskas verksamheten i krissituationen: vilka åtgärder genomfördes väl, var fanns det utrymme för förbättringar samt hur kan säkerhetsnivån och -planerna förbättras? Det är skäl att utarbeta en rapport om hanteringen av efterverkningarna som, förutom händelseförloppet, även inkluderar svar på åtminstone följande frågor:

- Grundorsaker till incidenten:
    - Vilka tekniska eller funktionsmässiga svagheter ledde till situationen?
- Det egna skyddets effektivitet:
    - Var de kontroller som användes för att upptäcka angrepp tillräckliga?
    - Orsakade angriparens handlingar några larm?
    - Hur reagerade man på larmen? Fick rätt ansvariga personer information om larmen?
- Agerande i krissituationen:
    - Följde man krisplanen? Hur användbar var den?
    - Fördelades krisgruppens ansvar mellan rätt personer?
    - Hur väl lyckades man begränsa angreppet och driva bort angriparen?
    - Hur väl lyckades krisgruppens kommunikation? Hur beaktades intressenterna?
- Återställande:
    - Hur väl lyckades man återställa kritiska uppgifter och tjänster?
- Efterverkningar:
    - Har händelseförloppet och utredningsarbetet dokumenterats?
    - Var den tekniska utredningen av incidenten tillräcklig? Har man kunnat förse till exempel myndigheterna med tillräckligt med material om angreppet?
    - Utvärdera tjänsteleverantörernas verksamhet. Var svarstiden och de avtalade tjänsterna tillräckliga för att utreda incidenten?

Efter incidenten ska organisationen uppdatera sin incidenthanteringsplan och sina mer detaljerade anvisningar för bekämpning av olika typer av avvikelser. Det rekommenderas även att organisationerna med jämna mellanrum övar på olika scenarier, så att nyttan med dem kan garanteras vid en krissituation.

Cybersäkerhetscentret önskar att företag och organisationer skulle dela med sig av de viktigaste lärdomarna som de dragit av incidenter. Med hjälp av fallrapporter kan Cybersäkerhetscentret hjälpa andra organisationer i Finland och utomlands vid utredningen av liknande fall. De lärdomar som återställandet ger bidrar till att utveckla beredskapen för alla organisationer.

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

kyberturvallisuuskeskus.fi

ISBN 978-952-311-813-3

FÖRSÖRJNINGS-
BEREDSKAPCENTRALEN

TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret