TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret

Anvisning – Dataintrång

Traficoms forskningsrapporter och utredningar
24/2022

Innehållsförteckning

1 Inledning 2
1.1 Syftet med anvisningen 2
1.2 Vad är ett dataintrång? 2
2 Beredskap 3
2.1 Administrativa åtgärder 3
2.2 Tekniska åtgärder 4
3 Upptäcka en informationssäkerhetsincident 5
4 Anvisningar 6
4.1 Arbetsflödet vid utredning av en informationssäkerhetsincident 6
4.2 Omedelbara åtgärder 8
4.3 Utredning av en informationssäkerhetsincident 10
4.4 Återställande 12
5 Efterverkningar av informationssäkerhetsincidenten 14

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 dataintrång. 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 dataintrång?

Dataintrång innebär olovligt intrång i ett datasystem, en tjänst eller en enhet, eller olovlig användning av en applikation med hjälp av koder som man kommit över. Med dataintrång försöker man ofta få ekonomiska fördela genom att till exempel stjäla information som man kan sälja vidare. Ibland stjäl den som gör intrånget själv ingenting, utan säljer tillträdet till servern till någon annan brottsling. En miljö som någon gjort intrång i kan även användas för att sprida skadligt material eller så kan miljöns funktion lamslås med utpressningsprogram. Angriparen kan använda miljön som en del av andra angrepp, till exempel överbelastningsangrepp.

Dataintrång orsakar ekonomiska förluster och förlust av anseende för den angripna organisationen. Dessutom kan organisationens normala verksamhet vara förhindrad också för en längre tid på grund av korrigerande åtgärder eller återinstallationer i miljön. Dataintrång används även för fakturabedrägerier (eng. Business Email Compromise), där de ekonomiska förlusterna kan vara stora. När en organisation faller offer för ett dataintrång skickas en förfalskad faktura inifrån organisationen, till skillnad från vanliga vd-bedrägerier, och därför är det mer sannolikt att den godkänns.

Ofta kan dataintrånget utnyttjas först långt efter själva intrånget. I sådana fall har organisationen inte nödvändigtvis längre kvar loggdata från tiden för intrånget, vilket försvårar utredningen av incidenten avsevärt.

2 Beredskap

Ett centralt sätt att minska incidenternas allvarlighetsgrad samt möjliggöra snabb återhämtning och att affärsverksamheten kan fortsätta är att förbereda sig för incidenter. 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 nätet 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 den eventuella 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 dataintrång.
- Utbilda personalen i hur den ska agera medan en sådan incident som beskrivs i anvisningen 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.
- Definiera noggrant vilka behörigheter som behövs för användarna och de tekniska funktionerna.
- 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.

[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

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 (eng. Network Segmentation), datakryptering och åtkomstbegränsning för att säkerställa att ditt företags angreppsyta och det material som åt gången är mottagligt för angrepp är så små som möjligt.
- 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 (eng. Endpoing Detection and Response, EDR), 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.
- Ta i bruk en centraliserad logghantering för att göra det möjligt att effektivt upptäcka och undersöka cyberrisker.

3 Upptäcka en informationssäkerhetsincident

Möjligheterna att upptäcka ett angrepp beror i hög grad på vilket sätt angriparen använt sig av för att ta sig in i systemet. Intrånget kan ha skett till exempel genom att angriparen utnyttjat en sårbarhet i en server, ett konfigurationsfel, en sårbarhet i en applikation eller så kan angriparen ha kommit över lämpliga koder till servern, till exempel genom nätfiske.

Ett angrepp kan upptäckas på till exempel följande sätt:

- Systemet slutar fungera eller är inte tillgängligt.
- Oväntade åtgärder har utförts i systemet som ingen av de anställda tror sig ha gjort.
- En informationssäkerhetsprodukt eller en tjänsteleverantör avger ett larm.
- Organisationen får ett meddelande om ett angrepp utifrån organisationen, till exempel via sociala medier, en kund, en samarbetspartner eller en myndighet.
- En allvarlig sårbarhet upptäcks i systemet och i samband med åtgärdandet framkommer det att sårbarheten redan har utnyttjats.
- Angriparen försöker utöva utpressning mot organisationen med hjälp av de stulna uppgifterna.

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

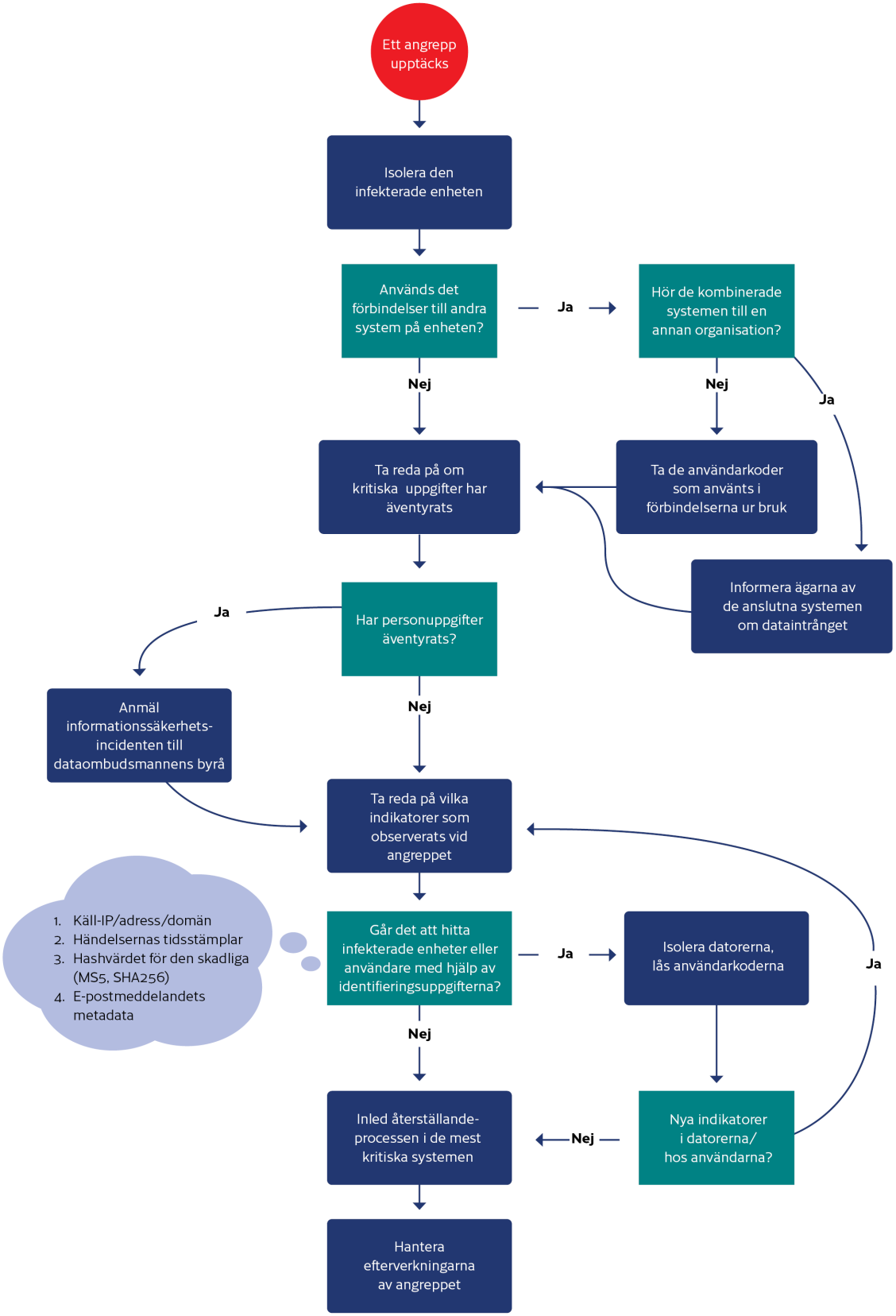
4 Anvisningar

Använd nedanstående checklista på åtgärder som hjälp när du misstänker att du fallit offer för ett dataintrång. 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.


Ett angrepp upptäcks
Isolera den infekterade enheten
Används det förbindelser till andra system på enheten?
Ja
Hör de kombinerade systemen till en annan organisation?
Nej
Ja
Nej
Ta reda på om kritiska uppgifter har äventyrats
Ta de användarkoder som använts i förbindelserna ur bruk
Informera ägarna av de anslutna systemen om dataintrånget
Ja
Har personuppgifter äventyrats?
Nej
Anmäl informationssäkerhets-incidenten till dataombudsmannens byrå
Ta reda på vilka indikatorer som observerats vid angreppet
1. Käll-IP/adress/domän
2. Händelsernas tidsstämplar
3. Hashvärdet för den skadliga (MS5, SHA256)
4. E-postmeddelandets metadata
Går det att hitta infekterade enheter eller användare med hjälp av identifieringsuppgifterna?
Ja
Isolera datorerna, lås användarkoderna
Ja
Nej
Inled återställande-processen i de mest kritiska systemen
Nej
Nya indikatorer i datorerna/ hos användarna?
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.	Isolera enheten med hjälp av funktionerna i den centraliserade övervakningen av enheterna. Dra vid behov ur enhetens nätverkskablar. Isoleringen måste även hindra enhetens tillgång till internet, så att angriparens möjligheter att stjäla information från servern stoppas.
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.	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 hjälpa till att lösa situationen.
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. Integriteten för kombinerade system ska säkerställas så fort som möjligt, så att man kan få en bild av hur allvarlig situationen är.	Om servern har anslutningar till andra system ska uppgifternas integritet säkerställas genom granskningar av de kombinerade systemens loggar. Det kan vara fråga om att kontrollera till exempel 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.
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.	Informera intressenternas kontaktpersoner vid krissituationer om incidenten om ni tror att den kan påverka tillgången till deras tjänster. Om det funnits anslutningar från servern till andra organisationer ska även dessa informeras. På så sätt kan de 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.
Bedöm om du behöver utomstående hjälp för att hantera informationssäkerhetsincidenten	Organisationen kan behöva hjälp med de tekniska åtgärderna, hanteringen av incidenten och organiseringen av åtgärderna. 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. Det kan krävas extern kompetens för till exempel insamling av identifieringsuppgifter och utredning av hotet utifrån dem. Den externa hjälpen kan även

		till exempel 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. I resurserna i fotnoten hittar du finländska tjänsteleverantörer.[8]
Anmäl informationssäkerhetsincidenten till dataombudsmannens byrå	Om det finns en risk för 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 personuppgiftsincidenten, eftersom anmälan kan kompletteras senare. Den personuppgiftsansvarige måste bedöma hur stor risk personuppgiftsincidenten orsakar 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 incidenten 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 (det så kallade NIS-direktivet), ska anmäla informationssäkerhetsincidenter i nätverks- och informationssystem till myndigheterna.[11]

[8] https://dfir.fi/
https://www.fisc.fi/fi
https://www.hansel.fi/sv/upphandlingar/tiedonhallinnan-ja-digiturvallisuuden-asiantuntija/

[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 grundlig utredning säkerställs att skadliga programvaror och eventuella bakdörrar har avlägsnats ur miljön.

Steg	Syfte	Åtgärder
Identifiera 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. Först när angriparen har körts bort från miljöerna kan återhämtningen börja.	Identifieringsuppgifter som ska samlas in är bland annat tidpunkten för olika händelser, till exempel när man har loggat in på servern eller när ett visst kommando har körts på servern. Den skadliga programvaran kommunicerar ofta med angriparens kommandoserver. Genom att kontrollera de infekterade enheternas nättrafik eller undersöka domännamnen (DNS-loggarna) kan de käll-IP-adresser eller domännamn som angriparen använder identifieras. När de skadliga filerna identifierats kan man ta reda på deras hashvärden (MD5/SHA256), med hjälp av vilka de skadliga filerna kan identifieras även på övriga enheter. Utifrån identifieringshändelser som riktats mot de infekterade enheterna och de åtgärder som utförts med användarkonton i anknytning till dessa kan man 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 ska de enskilda servrarnas och enheternas loggar undersökas.
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 man söka infekterade enheter, till exempel genom att använda funktionerna i den centraliserade övervakningen av enheterna, vilka ofta erbjuder möjlighet att söka händelser på enheterna med hjälp av olika identifikationskoder. Om organisationen även har en centraliserad logghantering kan man 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 enhet. För det kan man dock ännu 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 försökt dölja sina spår genom att koppla bort insamlingen av loggar. I sådana fall är det inte nödvändigtvis möjligt att hitta alla insamlade identifieringsuppgifter i enhetens loggar. Därför är det viktigt att försöka använda ett brett spektrum av olika slags identifieringsuppgifter och händelsekällor.
Ta reda på om kritiska uppgifter har äventyrats	Som en del av utredningen ska man ta reda på huruvida angriparen 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 om angriparen har kommit över och stulit uppgifter genom att övervaka loggarna för en databas eller ett gränssnitt. Utifrån belastningen eller de sökningar som gjorts kan du avgöra om angriparen har försökt hämta uppgifter. Kontrollera nätenheternas loggar för avvikelser i den infekterade serverns trafik. En exceptionellt stor mängd trafik kan vara ett tecken på till exempel att angriparen har lyckats stjäla information. Observera att angriparen kan ha ändrat data, även om han eller hon inte skulle ha förstört eller stulit dem. Angriparen kan även ha stulit små, men viktiga 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 brottsanmälan och för rättegångsförhandlingar. Om organisationen har en cyberförsäkring kan även försäkringsbolaget kräva närmare uppgifter om incidenten samt bevis för en utredning.	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 möjligt. Använd en hashfunktion för att säkerställa deras integritet. Sträva efter att spara bevis på de skadliga programvaror som upptäckts. Stor försiktighet ska iakttas vid hanteringen. En säker hantering 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	Inled återställandet 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
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. Beakta även risken för 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 har utnyttjat vid angreppet. Du kan försöka undvika risken genom att återställa systemen utan nätförbindelser samt uppdatera operativsystemet och dess applikationer innan du ansluter dem till nätet. 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 de inte nödvändigtvis kan rensa systemet fullständigt. Kontrollera systemen med programvaror 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 eventuellt 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. Använd inte organisationens e-post eller snabbmeddelanden, 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 återställandet, för den händelse att angriparen på nytt kommer över dem. Om det förblir oklart för organisationen hur angriparen kunde komma över vissa koder, överväg att skapa helt nya koder. På så sätt försäkrar du dig om att angriparen inte kommer över koderna på nytt på samma sätt.

Återställ infekterade poster	Om man misstänker att angriparen har ändrat innehåll i databasen ska databasen återställas från en säkerhetskopia för att annullera angriparens ändringar, ifall det inte är möjligt att rensa data.	Använd dig av databasens och gränssnittens loggar för att ta reda på huruvida angriparen har redigerat poster. Om loggarna inte är tillräckligt exakta för att rensa ändringarna ska databasens uppgifter återställas från den senaste säkra säkerhetskopian. Om angriparen har stulit information ska alla lösenord i den stulna informationen ändras. Detta ska göras även om lösenorden skulle ha lagrats endast i form av lösenordshashar. Informera de personer vars uppgifter har äventyrats i samband med intrånget, så att de kan förbereda sig på att deras uppgifter eventuellt kommer att missbrukas. Meddela även att man varit tvungen att återställa uppgifterna till en äldre version från och med ett visst datum, så att vederbörande kan uppdatera sina uppgifter.

5 Efterverkningar av informationssäkerhetsincidenten

När krisen är över och affärsfunktionerna normaliserat sig är det viktigt att börja hantera efterverkningarna av angreppet 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 ett liknande angrepp 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 978-952-311-816-4

FÖRSÖRJNINGS-
BEREDSKAPCENTRALEN

TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret