TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret

Anvisning – Utpressningsprogram

Traficoms forskningsrapporter och utredningar
23/2022

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 att ett angrepp med ett utpressningsprogram eller där ett utpressningsprogram hindrar den normala verksamheten. 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 utpressningsprogram?

Utpressningsprogram (eng. Ransomware) används vid cyberangrepp, där nätbrottslingar försöker dölja en organisations data med hjälp av en krypteringsalgoritm och kräver lösen för att lämna tillbaka uppgifterna. Ofta stjäl brottslingarna även konfidentiell information och kan utöva utpressning mot organisationen genom hot om dataläckage.

Utpressningsprogram har visat sig vara ett effektivt sätt för brottslingar att få ekonomiska fördelar, eftersom organisationer som inte är förberedda på hotet är lätta mål. Att betala lösen för att lösa situationen är dock inte den rätta lösningen. Betalning är inte nödvändigtvis en garanti för att uppgifterna lämnas tillbaka, och hindrar kanske inte ens att utpressningen eller andra angrepp fortsätter. Angriparen kan även ha som mål att endast förstöra data, vilket betyder att utpressningen endast är en bluff. I sådana fall är det inte möjligt att återställa data ens genom att betala lösensumman.

Rätt beredskap för angrepp med utpressningsprogram förbättrar avsevärt organisationernas informationssäkerhetsnivå och tålighet i förhållande till såväl utpressningsprogram som andra eventuella angrepp. Utöver denna anvisning har Cybersäkerhetscentret även publicerat en anvisning avsedd särskilt för ledningen i organisationer om hur de ska agera vid angrepp med utpressningsprogram.[1]

[1] https://www.kyberturvallisuuskeskus.fi/sv/publikationer/atgarder-vid-angrepp-med-utpressningsprogram-ledningens-anvisningar

2 Beredskap

Ett bra 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.[2] 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 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.[3] Beroende på vilka system en organisation använder, krävs vanligtvis dessutom lösningar på nätverks- och systemnivå för omfattande monitorering.

2.1 Administrativa åtgärder

Omedelbara åtgärder

- Upprätta en incidenthanteringsplan för din organisation för användning i händelse av angrepp med utpressningsprogram.
- Utbilda personalen i hur den ska agera vid en sådan incident som beskrivs i denna anvisning.
    - Erbjud även vanliga arbetstagare en grundläggande utbildning, där de får råd för hur de ska agera om ett utpressningsprogram angriper deras egen enhet.
- Ta i förväg reda på hur du kan anmäla en informationssäkerhetsincident till Cybersäkerhetscentret.[4] Följ Cybersäkerhetscentrets aktuella meddelanden.[5]
- Gå igenom olika angreppsscenarier tillsammans med ledningen och kom överens om praktiska åtgärder samt ledningsansvar och -befogenheter vid informationssäkerhetsincidenter.
- Öva på[6] 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.
- Överväg att teckna en cyberförsäkring för ditt företag som kan täcka skador till följd av angrepp med utpressningsprogram. Diskutera närmare detaljer med försäkringsbolagen. Berätta dock inte offentligt om din organisation har en cyberförsäkring, eftersom nätbrottslingar kan rikta angrepp just till sådana organisationer i hopp om att de mer sannolikt betalar lösen.

Åtgärder som främjar cybersäkerhet i ett bredare perspektiv

- Identifiera de komponenter som är kritiska för affärsverksamheten samt skapa och upprätta en förteckning över de objekt som ska skyddas.
- Se till att din organisation och dess underleverantörer har processer för kontinuerlig hantering av sårbarheter och uppdateringar.

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

[5] https://www.kyberturvallisuuskeskus.fi/sv/ajankohtaiset

[6] https://www.kyberturvallisuuskeskus.fi/sv/vara-tjanster/ovningar

- 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.

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 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.

2.3 Beredskap och övning i praktiken

En viktig del av beredskapen är även att öva på hotscenarier. Genom att öva på nedanstående scenario i förväg kan du säkerställa att din organisation är redo att möta en dylik situation. Genom att öva försäkrar sig organisationen bland annat om att personalen förstår vad punkterna i arbetsflödesschemat och checklistan i anvisningen betyder och att den har förmåga att agera enligt de anvisningar som beskrivs.

Scenariot i detta fall skulle till exempel kunna vara en situation, där ett utpressningsprogram har låst filerna i ett system som är kritiskt för verksamheten, samtidigt som det hindrar användningen av systemet och dess funktion. För organisationen visar sig detta i form av att systemet slutar fungera. Angriparna har tagit sig in i organisationen med hjälp av ett nätfiskemeddelande och via en infekterad arbetsstation lyckats ta sig in i ett kritiskt system genom att använda sig av en sårbarhet som funnits i servern. Personalen och kunderna belastar IT- och kundstödet, och trycket på att återställa verksamheten eller hitta alternativa verksamhetssätt ökar.

Hur skulle man i din organisation agera i en dylik situation? Försök att med hjälp av övning fördela tillräckligt med ansvar och resurser inom fyra parallella områden som är centrala för en snabb återhämtning:

1. Återgång till normaltillståndet (återhämtning)
2. Utredning av grundorsaken och förhindrande av ytterligare skador (utredning och korrigerande åtgärder)
3. Tillfälliga lösningar under återhämtningen och kontrollerad upplösning av dessa efter återhämtningen (eng. Workarounds/Stopgap Measures).

4. Kommunikation mellan det reagerande teamet, den övriga personalen, intressenter, ledningen och offentligheten, informering och samordning (samordning).

Öva på åtminstone följande steg i dessa anvisningar:

- Informera om incidenten och eskalera situationen.
- Blockera omedelbart de identifierade enheterna från nätverket.
- Lås infekterade koder och avbryt aktiva sessioner.
- Säkerställ verksamhetens kontinuitet medan informationssäkerhetsincidenten pågår.
- Samla in identifieringsuppgifter om den skadliga programvaran och logganalys.
    - Är det möjligt att ta reda på hur och varifrån den skadliga programvaran har kommit?
    - Vems användarkoder har blivit utsatta?
- Använd de insamlade identifieringsuppgifterna för att kontrollera om andra servrar och enheter är infekterade.
- Ta reda på vem som tagit emot nätfiskemeddelandet.
    - Vem har öppnat den skadliga bilagan?
- Återställ de infekterade systemen.
    - Servrar och enheter. Använd säkerhetskopior.
- Genomför en process för den slutliga utredningen av incidenten.

Vid sidan om alla uppgifter att öva på är det bra att tänka på hur organisationen leder hanteringen av incidenten, hur den interna kommunikationen fungerar samt vem som i vilket skede är ansvariga personer och vem deras ersättare är. Organisationer rekommenderas även ta del av Cybersäkerhetscentrets material om övningar.[7]

[7] https://www.kyberturvallisuuskeskus.fi/sv/vara-tjanster/ovningar

3 Upptäcka en informationssäkerhetsincident

Det finns två typer av angrepp: utpressningsangrepp (ransomware) och angrepp i syfte att förstöra (wiperware). Konsekvenserna är desamma i båda fallen: du kommer inte åt filer eller system som är viktiga för din organisations verksamhet. Ett angrepp kan upptäckas på till exempel följande sätt:

- Angriparen skickar ett utpressningsmeddelande till målorganisationen eller ett sådant dyker upp på skärmen vid en arbetsstation.
- Organisationen får ett meddelande om ett angrepp utifrån organisationen, till exempel via sociala medier, en kund, en samarbetspartner eller en myndighet.
- Organisationens filer kan inte öppnas exempelvis i en webbaserad databas eller så är de på annat sätt oanvändbara.
- Utrustning i fabriks- eller produktionsmiljön slutar fungera utan någon synlig eller identifierbar orsak.
- En informationssäkerhetsprodukt eller en tjänsteleverantör avger ett larm.

Anmäl informationssäkerhetsincidenten till Cybersäkerhetscentret.[8] 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 andra eventuella offer.

Läs Cybersäkerhetscentrets anvisning för hur man upptäcker dataintrång (på finska).[9]

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

[9] https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/opas-tietomurtojen-havaitsemiseen

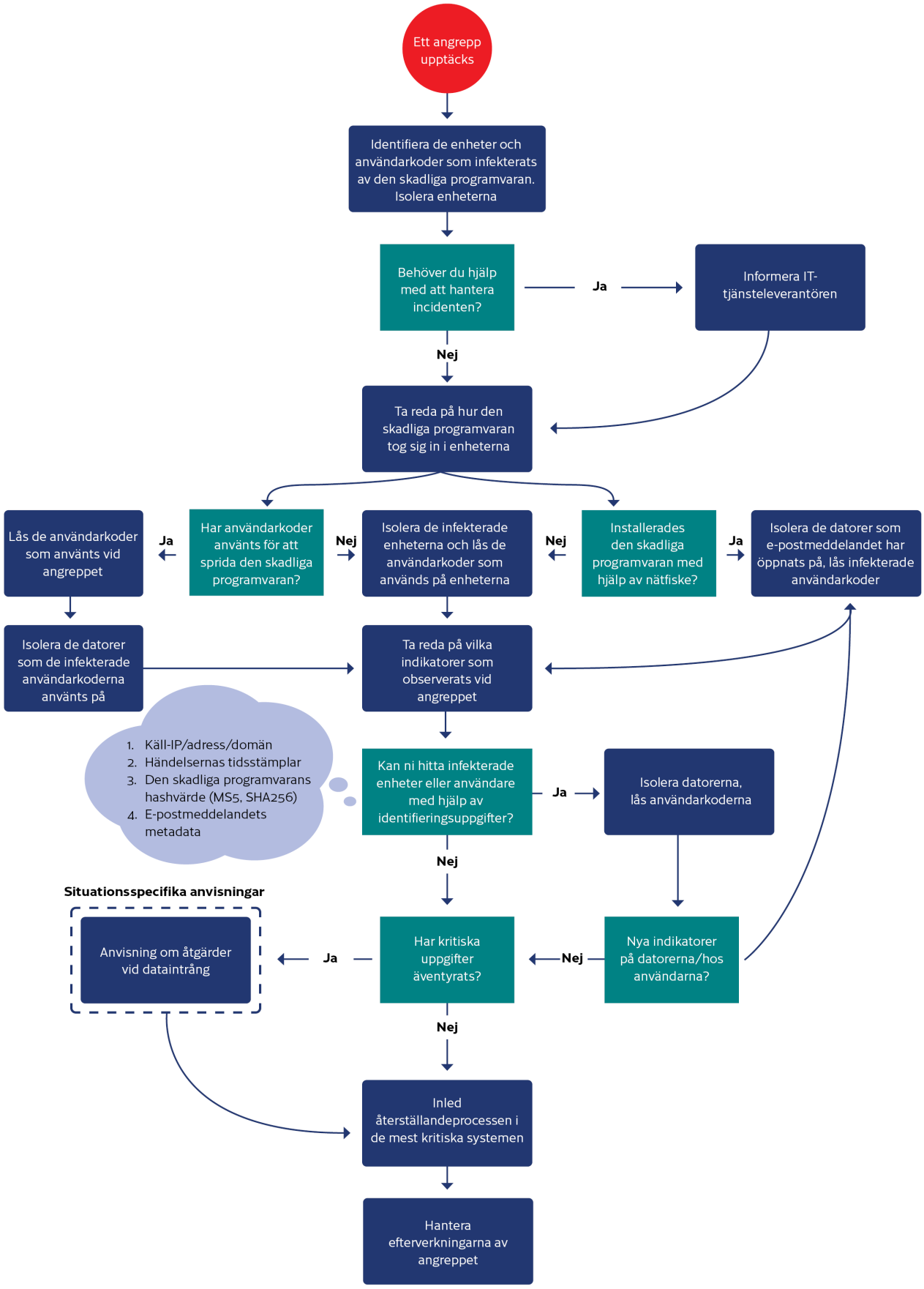
4 Anvisningar

Använd nedanstående checklista på åtgärder som hjälp när du misstänker att du fallit offer för ett utpressningsprogram. 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
Identifiera de enheter och användarkoder som infekterats av den skadliga programvaran. Isolera enheterna
Behöver du hjälp med att hantera incidenten?
Ja
Informera IT-tjänsteleverantören
Nej
Ta reda på hur den skadliga programvaran tog sig in i enheterna
Lås de användarkoder som använts vid angreppet
Ja
Har användarkoder använts för att sprida den skadliga programvaran?
Nej
Isolera de infekterade enheterna och lås de användarkoder som används på enheterna
Nej
Installerades den skadliga programvaran med hjälp av nätfiske?
Ja
Isolera de datorer som e-postmeddelandet har öppnats på, lås infekterade användarkoder
Isolera de datorer som de infekterade användarkoderna använts på
Ta reda på vilka indikatorer som observerats vid angreppet
1. Käll-IP/adress/domän
2. Händelsernas tidsstämplar
3. Den skadliga programvarans hashvärde (MS5, SHA256)
4. E-postmeddelandets metadata
Kan ni hitta infekterade enheter eller användare med hjälp av identifieringsuppgifter?
Ja
Isolera datorerna, lås användarkoderna
Nej
Situationsspecifika anvisningar
Anvisning om åtgärder vid dataintrång
Ja
Har kritiska uppgifter äventyrats?
Nej
Nya indikatorer på datorerna/hos användarna?
Nej
Inled återställandeprocessen i de mest kritiska systemen
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 stoppa spridningen av den skadliga programvaran, hindra angriparna från att få fotfäste i nätverket och förbereda inledningen av återhämtningsprocessen. Ge inte efter för angriparnas utpressning. Att betala lösen garanterar inte att situationen löser sig eller att uppgifterna lämnas tillbaka.

Steg	Syfte	Åtgärder
Identifiera infekterade system och användarkoder	Målet är att identifiera alla servrar och enheter som utpressningsprogrammet har hunnit sprida sig till. Utöver detta försöker man även identifiera de användarkoder som angriparen kan ha kommit över.	Använd dina övervakningsprodukter för att identifiera vilka enheter och koder som är infekterade. Kontrollera vilka användare som varit inloggade på de infekterade enheterna och ta reda på vilka andra ställen de varit inloggade på. Detta kan du göra bland annat utifrån Active Directory-loggar, med hjälp av en centraliserad övervakningsprodukt för enheterna (eng. Endpoint Detection and Response) eller i loggarna för identitetshanteringen.
Blockera de infekterade enheter som identifierats	Genom att blockera de infekterade enheterna som identifierats från alla datanät kan man lyckas hindra angreppet från att sprida sig.	Blockera enheterna genom att använda dig av funktionerna i den centraliserade övervakningen av enheterna. Dra vid behov ur enheternas nätverkskablar. Lämna enheterna påslagna efter blockeringen. Det gör det möjligt att återställa dem om de krypteringsnycklar som utpressningsprogrammet använt fortfarande finns i minnet. Minnesbaserad undersökning är även ett effektivt sätt att reda ut informationssäkerhetsincidenter.
Identifiera de användarkoder som använts vid angreppet	Ofta sprids skadliga programvaror med hjälp av användarkoder med bred åtkomst (till exempel administratörskoder).	Undersök i övervakningsprodukten för enheterna eller i de infekterade enheternas loggar hur den skadliga programvaran har tagit sig in i enheterna. Alla koder som använts för inloggning på infekterade servrar och enheter ska betraktas som förlorade. Observera även lokala koder och servicekoder till servrar och enheter (eng. Service Accounts) som angriparen kan ha kommit över. Angriparna använder ofta verktyg (till exempel Mimikatz) för att stjäla koder som finns i enheternas minne. Det är därför skäl att låsa även dessa koder.
Kontakta din IT-tjänsteleverantör	Ofta har en del av organisationers IT-infrastruktur utkontrakterats till en tjänsteleverantör. I sådana fall kan åtgärder för att begränsa incidenten 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 hjälpa till att lösa incidenter.
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. Ett angrepp mot leveranskedjan kan även äventyra samtliga partners säkerhet.	Informera intressenternas kontaktpersoner vid krissituationer om incidenten om du tror att den kan påverka deras data och tillgången till tjänsterna, eller om det finns en risk för att den skadliga programvaran kan sprida sig mellan organisationerna. Det är en god idé att informera aktivt om incidenten även internt. Om den skadliga programvaran redan har fått stor spridning kan det vara bra att instruera de anställda att undvika att starta sina datorer för att förhindra följdskador.
Bedöm om du behöver utomstående hjälp för att hantera informationssäkerhetsincidenten	Organisationen kan behöva hjälp med att organisera åtgärder, hantera incidenten och utföra tekniska åtgärder. Om det inte finns tillräcklig kompetens i den egna organisationen eller hos IT-tjänsteleverantören ska man överväga att anlita hjälp utifrån.	De tekniska åtgärderna vid hanteringen av en incident kan kräva extern kompetens. Sådana åtgärder kan vara bland annat insamling av identifieringsuppgifter, utredning av hotet utifrån dem, identifiering av typen av utpressningsprogram och analys av de infekterade datorernas minnen. 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.[10]
Rapportera informationssäkerhetsincidenten till myndigheterna	Rapportera incidenten till myndigheterna. Organisationen kan enligt författningar eller en cyberförsäkring vara skyldig att anmäla incidenten.	Gör en brottsanmälan om händelsen till polisen.[11] Anmäl händelsen även till Cybersäkerhetscentret[12] för att upprätthålla lägesbilden och få hjälp. Om det finns en risk för att personuppgifter eller andra uppgifter som omfattas av dataskyddslagstiftningen (GDPR) har hamnat i händerna på angriparen, gör en anmälan till dataombudsmannens byrå.[13] Aktörer och tjänsteleverantörer, som är kritiska med tanke på försörjningsberedskapen och som omfattas av EU:s direktiv

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

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

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

[13] https://tietosuoja.fi/sv/anmalan-om-personuppgiftsincident

		om säkerhet i nätverks- och informationssystem (det så kallade NIS-direktivet), ska anmäla informationssäkerhetsincidenter i nätverks- och informationssystem till tillsynsmyndigheterna.[14]

[14] 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 omsorgsfull utredning säkerställs att skadliga programvaror, behörigheter som hamnat i fel händer 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 tidpunkterna 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. Om den skadliga programvaran ursprungligen har skickats till organisationen per e-post eller via något annat kommunikationsmedel ska identifieringsuppgifter samlas in om meddelandena. Viktiga uppgifter om meddelandena är tidsstämplar, ämnen, bilagor, avsändare, mottagare och innehåll. Med hjälp av dessa uppgifter kan man ta reda på vem alla som eventuellt har tagit emot det skadliga meddelandet och via det fått den skadliga programvaran på sin dator.
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 en direkt möjlighet att med olika identifikationskoder söka händelser på enheterna.

		Om organisationen även har en centraliserad loggserver kan man i den effektivt söka händelser på 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 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.
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 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.[15]

[15] 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 helt från början. Beakta även de riskfaktorer som nämns i föregående kapitel. Försök inte rensa ett infekterat system med automatiska verktyg eller antivirusprogram, eftersom det inte finns några garantier för att de kan rensa systemet fullständigt. Spara de krypterade filerna eller hårddiskarna, utifall att ni i ett senare skede skulle hitta ett sätt att öppna dem. 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. 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. Om organisationen använder sig av Active Directory och man misstänker att angriparen i något skede kommit över hela domänen, ändra även lösenordet för KRBTGT-kontot två gånger för att göra så att förfallotiden för en så kallad Golden Ticket löper ut. Konfigurera även Active Directory-certifikattjänster (eng. Certificate Services) på nytt, utifall att angriparen har kommit över certifikat i certifikattjänsten som kan användas för identifiering.

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 978-952-311-815-7

FÖRSÖRJNINGS-
BEREDSKAPCENTRALEN

TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret