TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret

Åtgärder vid angrepp med utpressningsprogram - ledningens anvisningar

Traficoms
publikationer

15/2022

Innehållsförteckning

1 Vad handlar det om?

Ett utpressningsprogram eller en utpressningstrojan (eng. ransomware) är ett cyberangrepp där angriparna försöker dölja en organisations data med hjälp av en krypteringsalgoritm och kräver lösen för att lämna tillbaka uppgifterna. Brottslingarna kan även stjäla uppgifterna som de dolt och utöva utpressning mot er organisation genom hot om dataläckage. Risken för att råka ut för angrepp har ökat avsevärt under den senaste tiden: från år 2020 till år 2021 ökade antalet angrepp med omkring 105 procent.[1]

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 är dock inte alltid lösningen, eftersom angreppet och utpressningen till följd av det kan fortsätta trots betalningen. Rätt beredskap för angrepp med utpressningsprogram förbättrar avsevärt organisationernas informationssäkerhetsnivå och tålighet i förhållande till såväl utpressningsprogram som andra eventuella angrepp. Det är bra att notera att en del angrepp kan genomföras även i syfte att förstöra data.

Syftet med denna anvisning är att ge den högsta ledningen i organisationer vägledning för hur de ska agera vid angrepp med utpressningsprogram. Utöver denna anvisning behöver ni tekniska anvisningar för de personer som ansvarar för organisationens informationssäkerhet eller ICT-miljö. Exempel på tekniska anvisningar finns i kapitel 5 (Källor och ytterligare anvisningar). Bild 1 visar en sammanfattning av anvisningens innehåll om beredskapen för och hanteringen av angrepp ur ett helhetsperspektiv.

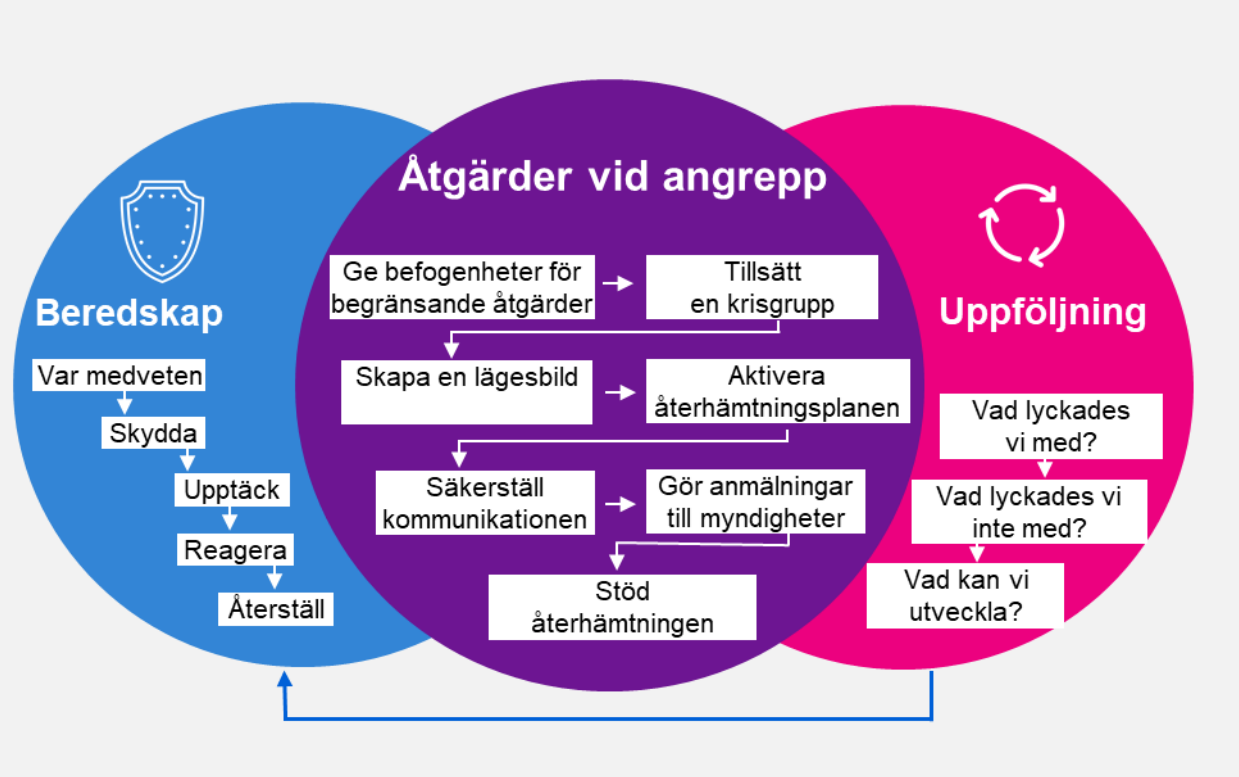

Bild1: Beredskap för och hantering av angrepp med utpressningsprogram ur ett helhetsperspektiv

1.1 Konsekvenser av angrepp

Ett lyckat angrepp med ett utpressningsprogram leder ofta till att affärsverksamheten störs eller till och med avbryts helt och hållet. Det kan innebära stora ekonomiska förluster för organisationen och dess kunder om man inte lyckas återupprätta verksamheten tillräckligt snabbt. I värsta fall kan skadeprogram via gemensamma tjänster tränga in också i fabriks- och

[1] Sonicwall, 2022 Sonicwall cyber threat report, https://www.sonicwall.com/medialibrary/en/white-paper/2022-sonicwall-cyber-threat-report.pdf

produktionsmiljöer samt deras affärssystem. Ett skadeprogram som tagit sig in i automationsmiljö kan stoppa produktionen helt och hållet eller i värsta fall utgöra ett säkerhetshot mot människorna eller miljön. Utöver ovanstående kan även vissa sanktioner som hänför sig till regleringen (inklusive dataskyddet) vara betydande till sin omfattning[2].

Ett angrepp med utpressningsprogram är ett hot mot företagets rykte, eftersom incidenter ofta leder till offentlig behandling. Detta kan ha stor inverkan även på organisationens rykte, förtroendet från olika intressenter och eventuellt på företagets värde, om organisationen inte har förberett sig för angreppet eller hanterat det på lämpligt sätt.

1.2 Hur kan ett angrepp starta?

Bild 2 visar ett möjligt scenario för hur angripare kan genomföra ett angrepp med utpressningsprogram. Det finns även många andra sätt att starta och genomföra angrepp.

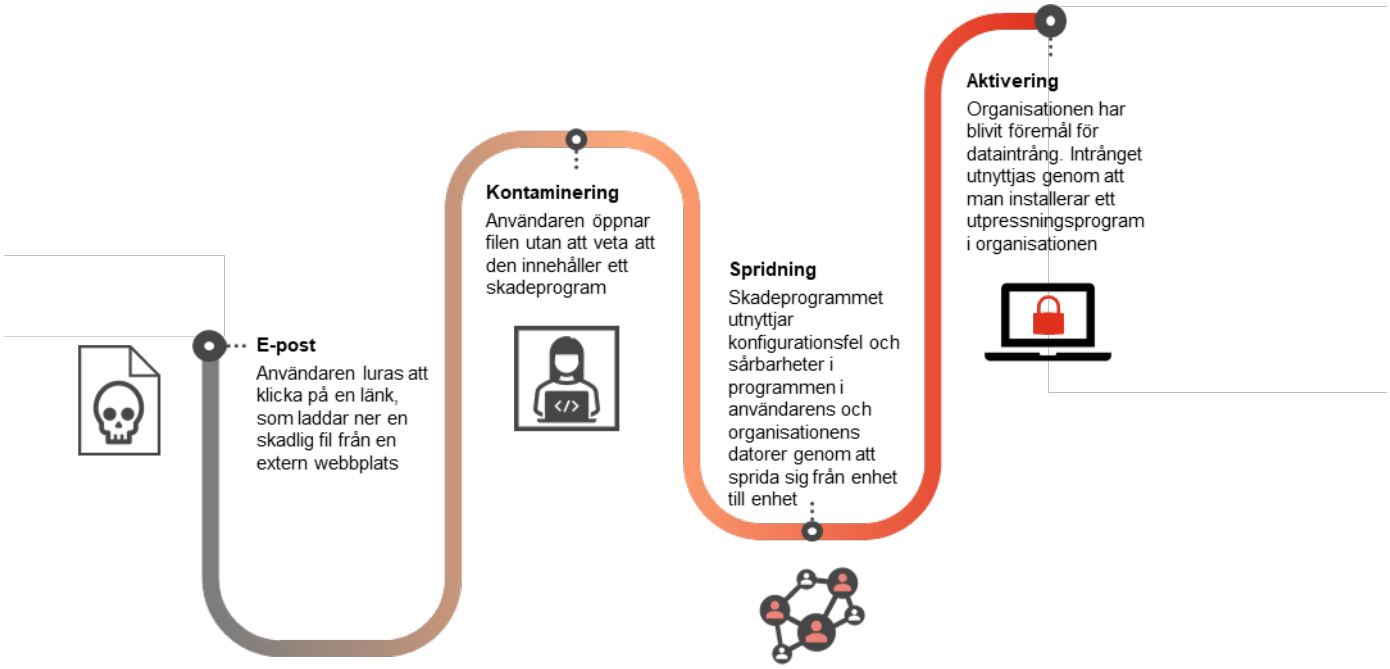

Bild 2: Ett exempel på ett angrepp med utpressningsprogram

1.3 Hur angrepp eventuellt visar sig

Angrepp med utpressningsprogram kan visa sig på olika sätt beroende på hur de genomförs. I bästa fall kan en organisation som utsätts för ett angrepp snabbt upptäcka de inledande skedena av angreppet och reagera på situationen på lämpligt sätt genom att hindra det från att sprida sig. I värsta fall upptäcks angreppet först när skadeprogrammet har spridit sig till nästan hela organisationen. Angripare har ofta som mål att genom sina åtgärder driva målorganisationen till en situation som känns hopplös och på så sätt försvåra återhämtningen från angreppet.

Det är ofta omöjligt för organisationens ledning att på egen hand hantera eller identifiera de olika sätt som ett angrepp kan manifestera sig på, men det är bra för ledningen att förstå när organisationen eventuellt har blivit föremål för ett angrepp med utpressningsprogram. Följande iakttagelser kan vara exempel på ett lyckat angrepp med utpressningsprogram:

- 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.

[2] GDPR.EU, What are the GDPR fines? 2022, https://gdpr.eu/fines/

- Organisationens filer kan inte öppnas exempelvis i en webbaserad databas eller så är de på annat sätt korrupta.
- Utrustning i fabriks- eller produktionsmiljön slutar fungera utan någon synlig eller identifierbar orsak.

2 Om det värsta skulle hända, gör så här!

2.1 Ge tillstånd och befogenheter för begränsande åtgärder

När ett angrepp med utpressningsprogram sker behövs snabba och beslutsamma åtgärder från ledningen, eftersom organisationen övergår från normal ledning till krisledning. Detta innebär samtidigt att befogenheterna att genomföra akuta begränsande åtgärder överförs från de normala befogenhetsprocesserna till ICT- eller informationssäkerhetspersonalen.

När det gäller att begränsa konsekvenserna av ett angrepp med utpressningsprogram har de första minuterna störst betydelse. ICT- eller informationssäkerhetspersonalen kan vara tvungen att fatta tuffa beslut, såsom att köra ner en del tjänster eller koppla bort dem från nätverket. Det är viktigt att ge dem befogenheter att på egen hand genomföra nödvändiga begränsande åtgärder, eftersom det i ett kritiskt läge kan ta för lång tid och förvärra problemet ytterligare om man ger befogenheter för en åtgärd i taget. Organisationen kan även behöva hjälp av externa experter. Även befogenheterna att anlita hjälp utifrån ska därför vara i ordning.

Det är bra om organisationens ledning är medveten om att experterna strävar efter att göra allt som krävs och att det är mycket viktigt att ge dem arbetsro samt säkerställa förutsättningarna för deras arbete under hela angreppet.

2.2 Tillsätt en krisgrupp

När ett angrepp sker är det viktigt att tillsätta en krisgrupp. Krisgruppens uppgift är att fördela ansvaret för och samordna de nödvändiga åtgärderna på organisationsnivå samt se till att genomförandet av de överenskomna begränsande åtgärderna eller lösningarna och deras effektivitet följs upp.

Krisgruppen kan vara till exempel organisationens ledningsgrupp i utökad sammansättning, men det skulle vara bra om den bestod av följande personer eller roller:

- Verkställande direktören
- En person som ansvarar för affärs- eller kärnfunktionerna
- En informationssäkerhetsansvarig
- En ICT-ansvarig
- En kommunikationsansvarig
- En person som ansvarar för juridiska frågor och/eller dataskyddet.

2.3 Krisgruppens uppgifter

2.3.1 Skapa en lägesbild

När er ICT- eller informationssäkerhetspersonal har satt igång de omedelbara begränsande åtgärderna och informerat organisationens ledning om läget ska krisgruppen göra upp en lägesbild av konsekvenserna av angreppet utifrån den information som är tillgänglig.

Beakta följande när ni skapar en lägesbild på organisationsnivå:

- Vad har den information som gått förlorad i angreppet för betydelse för och direkt effekt på er organisation samt på era kunders kärnfunktioner, affärsfunktioner eller stödfunktioner?
- Vilka ekonomiska följder ger situationen direkt eller indirekt upphov till och har er organisation tillräckligt med tillgängliga medel?
- Vem borde i första hand få information om angreppet (de anställda, styrelsen, kunderna, intressenterna)?
- Identifiera även eventuella andra scenarier som kan uppstå till följd av angreppet och sannolikheten för dem, till exempel har organisationen kanske utsatts för dataintrång eller hurdana följder skulle det ha för er eller era kunder om den information som stulits i samband med angreppet publiceras?
- Krisgruppen ska sörja för att en händelsedagbok (händelselogg) förs. Dokumentera noggrant angreppet och varje skede av återhämtningen efter det på en tidslinje. Utförlig dokumentation är mycket viktig med tanke på återhämtningen, lärdomarna av incidenten, det egna rättsskyddet och samarbetet med myndigheterna.

Krisgruppen har även till uppgift att se till att lägesbilden kontinuerligt uppdateras, så att det är möjligt att leda situationen och informera om den.

2.3.2 Planera och aktivera en återhämtningsplan

Om er organisation redan har en plan för återhämtningen efter incidenter med utpressningsprogram är det nu dags att börja agera enligt den.

Om er organisation inte har en plan ska ni fokusera på följande saker:

- Hur begränsar ni angriparens verksamhet och spridning i era informationssystem?
- Innan ni påbörjar återställandet, har angriparens förbindelser med era system brutits och har skadeprogrammen som installerats där tagits bort?
- Hur återställer ni era kärntjänster och er affärsverksamhet samt de resurser som dessa behöver till normalläge och hur säkerställer ni informationssäkerheten i dem?
- Vilka resurser (interna och externa) behöver ni för detta? Se till att ICT- eller informationssäkerhetspersonalen får det stöd den behöver under processen att återställa systemen, såsom vid granskning och återställande av säkerhetskopior.
- Om er organisation har en cyberförsäkring ska ni se till att organisationen kontaktar försäkringsbolaget. En del cyberförsäkringar kan innehålla tjänstekomponenter, såsom nödvändigt expertstöd, som kan vara till hjälp när situationen ska lösas.

Betala inte lösen! Till en början kan det verka som att kostnaderna som betalningen av lösensumman medför skulle vara mindre än vad det kostar att lösa krisen på egen hand. På grund av följande ska man dock under inga omständigheter betala lösen:

- Det går inte att lita på vad en brottsling säger, och det finns inga garantier för att de dekrypteringsnycklar som brottslingarna erbjuder fungerar.
- Även med fungerande nycklar kan återhämtningen vara långsam och dyr.
- Betalning av lösen finansierar brottslig verksamhet och bidrar till dess utveckling.
- Utpressningen kan också vara en bluff, och skadeprogrammet kanske förstör filerna istället för att kryptera dem.[3]

[3] https://www.bleepingcomputer.com/news/security/beware-onyx-ransomware-destroys-files-instead-of-encrypting-them/

- Betalning av lösen kan strida mot sanktionsregler eller den nationella lagstiftningen i det land som tar emot betalningen, det vill säga det kan även vara osäkert om betalningen av lösen går igenom.

2.3.3 Säkerställ den interna och externa kommunikationen

Planera hur ni ska informera bolagets styrelse, kunder, samarbetspartner och vid behov myndigheterna om situationen och återhämtningsprocessen samt hur den framskrider. Rapportera om och uppdatera lägesbilden till intressenter även i takt med att situationen framskrider.

Kom överens om vem som är organisationens officiella ansikte utåt och vem som kontaktar kunderna eller andra nödvändiga intressenter. Undvik en situation där de personer som har störst betydelse för lösningen av situationen (till exempel de tekniska experterna eller den informationssäkerhetsansvariga) är organisationens informatörer. De ska ges fullständig arbetsro för uppgifter som anknyter till återhämtningen efter incidenten.

2.3.4 Gör nödvändiga anmälningar till myndigheter

Anmäl angreppet till Cybersäkerhetscentret. Hos oss får ni hjälp med återhämtningen efter ett angrepp, och er anmälan hjälper andra organisationer som blir föremål för eventuella angrepp. Anmälan kan göras per e-post till cert@traficom.fi eller med en blankett (https://www.kyberturvallisuuskeskus.fi/sv/anmal). Var även beredda på att Cybersäkerhetscentret kontaktar er.

Gör en brottsanmälan om angreppet till polisen på https://asiointi.poliisi.fi/. Det är värt att göra en sådan i samband med den tekniska utredningen av angreppet, eftersom bevis ska fogas till anmälan. Polisen ger vägledning för hur ni tar tillvara bevismaterial på lämpligt sätt. Om angreppet äventyrar den allmänna säkerheten (till exempel ett säkerhetshot[4]), liv eller hälsa ska anmälan göras direkt till nödnumret 112.

Om brottslingarna har kommit över personuppgifter ska en anmälan göras till dataombudsmannens byrå på https://tietosuoja.fi/sv/anmalan-om-personuppgiftsincident inom 72 timmar från det att personuppgiftsincidenten upptäcktes. Det primära syftet med detta är att trygga den registrerades rättigheter. Ni kan vid behov göra anmälan stegvis: gör först en preliminär anmälan och komplettera den senare. [5]

Om er organisation verkar inom en bransch som är kritisk med tanke på försörjningsberedskapen ska angreppet anmälas även till tillsynsmyndigheten inom er bransch, i detta fall till en så kallad NIS-myndighet:
https://eservices.traficom.fi/dataservices/forms/NISlomake.aspx?langid=sv&RetUrl=https%3A//www.traficom.fi/sv/vara-tjanster. Mer information om bestämmelserna i NIS-direktivet finns här: https://www.kyberturvallisuuskeskus.fi/sv/var-verksamhet/reglering-och-tillsyn/digitala-tjanster-och-digital-infrastruktur

2.4 Främja genomförandet av återhämtningsplanen

När de omedelbara åtgärderna för att stoppa angreppet har inletts borde organisationens ledning fokusera på att främja återhämtningen genom nödvändiga åtgärder. Organisationens ledning kan göra detta genom att vara lättillgänglig för nyckelpersonerna, stödja arbetet för de personer som är centrala för återhämtningen samt bland annat upprätthålla en lugn och framåtblickande atmosfär. Det är bra att komma ihåg att det i det här skedet inte är skäl att fokusera på vad var och en kanske hade gjort fel eller låtit bli att göra.

Generellt sett ska man inte i det här skedet lägga för mycket vikt vid kostnaderna för återhämtningen efter angreppet eller den tid som gått förlorad på grund av det. Det viktigaste

[4] Säkerhetshot vid hantering av kemikalier: https://tukes.fi/turvauhkiin-varautuminen-vaarallisten-kemikaalien-kasittelyssa-ja-varastoinnissa (på finska)

[5] https://www.suomi.fi/guider/dataintrang/akuta-atgarder/informera-myndigheterna

är att som organisation försöka återhämta sig på ett så effektivt sätt som möjligt från angreppet, så att organisationen så snabbt som möjligt kan återgå till det normala.

3 Åtgärder efter krisen

När krisen är över och affärsfunktionerna normaliserat sig är det viktigt att börja hantera efterverkningarna av angreppet och att lära sig så mycket som möjligt av det inträffade. I samband med detta är det bra att med tanke på angreppet bedöma vad ni lyckades och inte lyckades med samt hur ni kan förbättra er säkerhetsnivå för att förhindra att något liknande inträffar i framtiden.

I första hand ska er organisation dock reda ut var angriparna tog sig in i era informationssystem och hur de avancerade i dem. Dessa brister eller bristfälliga säkerhetslösningar som möjliggjorde angreppet ska åtgärdas utan dröjsmål, så att något liknande angrepp inte kan upprepas. Till hjälp för utredningsarbetet är det bra att använda händelsedagboken som beskrivs i punkt 2.3.1 och som har kompletterats i takt med att utredningen och återhämtningen framskridit.

Efter det ska ni kartlägga er organisations förmåga att göra iakttagelser som hänför sig till angrepp. Försök hitta svar på nedanstående frågor tillsammans med era experter eller tjänsteleverantörer. Utifrån svaren ska ledningen se över organisationens observations- och hanteringsplaner samt processer, och försöka göra dem effektivare.

- Är era kontroller för att upptäcka angrepp tillräckliga?
- Orsakade angriparens handlingar några larm? Hurdana larm?
- Fick rätt personer information om larmen?
- Hurdana reaktioner fick dessa larm, om de gav upphov till några reaktioner?

Även återhämtningsprocessens effektivitet ska bedömas med hjälp av följande frågor:

- Fördelades krisgruppens ansvar mellan rätt personer? Hur klarade personerna i fråga av sina uppgifter?
- Hur väl lyckades IT-personalen vid återhämtningen? Kunde tjänsterna återställas i funktionsdugligt skick tillräckligt snabbt och räckte resurserna till?
- Lyckades krisgruppen kommunicera om rätt saker, till rätt personer och i rätt tid?
- Innehåller dokumentationen alla viktiga händelser med tanke på incidenten och är tidsstämplarna korrekta?
- Var den tekniska utredningen av incidenten tillräcklig?
- Hade bolagets ledning ett tillräckligt övergripande angreppssätt under själva situationen eller i beredskapen för den?

Även om angrepp med utpressningsprogram alltid är allvarliga, är det också möjligt att hantera dem. Det lyckas dock inte utan lämplig beredskap och ett fortlöpande arbete för att garantera cybersäkerheten.

4 Beredskap för hot

Angreppssätten utvecklas ständigt och därför måste arbetet för att säkerställa beredskapen för angrepp vara fortlöpande samt basera sig på systematisk verksamhet och ett försvar i olika skikt. Organisationens ledning ska avsätta nödvändiga resurser för angrepp med utpressningsprogram, så att säkerheten i det datanät och den servicemiljö som organisationen använder kan garanteras. Man bör även mäta huruvida resurserna är tillräckliga och huruvida beredskapsåtgärderna är effektiva i praktiken för att möjliggöra utveckling.

Fokus för cybersäkerheten ska ligga på försvarsmässigt djup och beredskapsförmåga på olika kontrollnivåer. Om ett försvarsskikt ger vika ger de övriga skikten ytterligare skydd. Beredskapen för utpressningsprogram kan delas in i fem olika skikt, som i kombination med varandra avsevärt förbättrar skyddet. Bild 3 visar även den ungefärliga betydelsegraden av respektive skikt i procent under hela beredskapsprocessen. Det är viktigt att förstå att en lämplig cyberberedskap lyckas endast i denna form och att enbart ett enskilt skyddande skikt ofta inte är tillräckligt.[6]

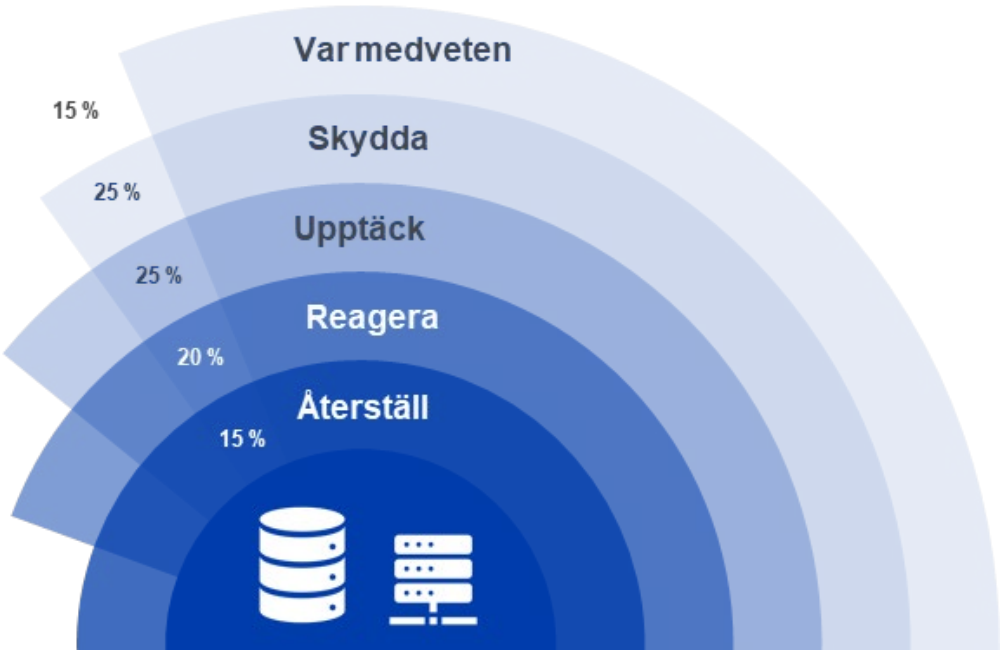

Bild 3: Beredskap för hot och betydelsen av olika delområden i beredskapsprocessen

4.1 Var medveten

Varje organisation är ett potentiellt mål för angrepp med utpressningsprogram, antingen direkt eller som en del av en kritisk leveranskedja. Brottslingarna kan även mycket noggrant anpassa sina angrepp och krav på lösen efter målorganisationen för att maximera sin vinst. Ta därför hotet på allvar.

Identifiera vilka tjänster som är livsviktiga för er verksamhet och bedöm vad som skulle hända om någon eller samtliga av dem inte skulle vara tillgängliga. Kartlägg därefter i samarbete med era ICT-experter den IT-egendom som er organisation använder och som ni behöver för att producera eller genomföra de tjänster som är centrala för er verksamhet. Sådan egendom är bland annat arbetsstationer, servrar, mobila enheter, databaser och användarregister. Kom ihåg att ni inte kan skydda er mot sådant som ni inte vet att existerar. Detta är till hjälp för er organisation även vid upprättandet av planer för avvikelsehantering och återhämtning.[7]

[6] NIST, Cybersecurity framework, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[7] https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf

Skapa därefter en kontext för beredskapens olika skikt genom att bedöma i synnerhet den risk som ett angrepp med utpressningsprogram eventuellt skulle utgöra. Beakta de befintliga administrativa och tekniska kontrollerna samt personalens medvetenhet i bedömningen. Kom ihåg att hantera de kvarstående riskerna och spegla dem mot er organisations risktagningsförmåga och riskbenägenhet. Diskutera hotet och risken med utpressningsprogram vid ledningsgruppens och styrelsens sammanträden.

Fastställ även serviceproducenternas ansvar och uppgifter genom avtal och krav.

Följ upp läget för de beredskapsåtgärder som ni använder och er organisations risknivå med hjälp av indikatorer som tagits fram för detta ändamål.

Det är viktigt för organisationens ledning att också tänka på att en tillräcklig andel av budgeten ska anvisas för cybersäkerhet för att tillräckliga beredskapsåtgärder ska kunna genomföras. Ni kan använda er av en tankemodell där ni bedömer hur stora ekonomiska förluster en investering i säkerheten skulle kunna förhindra i framtiden om den genomförs. Hur mycket skulle med andra ord ett eventuellt lyckat angrepp kosta er i euro? Detta gör det möjligt för er att även bedöma er organisations riskbenägenhet.

4.2 Skydda

Skyddsåtgärderna ska genomföras omsorgsfullt, eftersom det varje dag sker angreppsförsök via nätet. En del av dessa försök är inte värre än att er organisations nättjänster kan avvärja dem, men bland dem kan det även finnas mycket fientliga och aggressiva angreppsförsök. Med hjälp av ett effektivt skydd kan er organisation avvärja majoriteten av angreppsförsöken, men det kräver satsningar på underhållet och utvecklingen av cybersäkerheten.

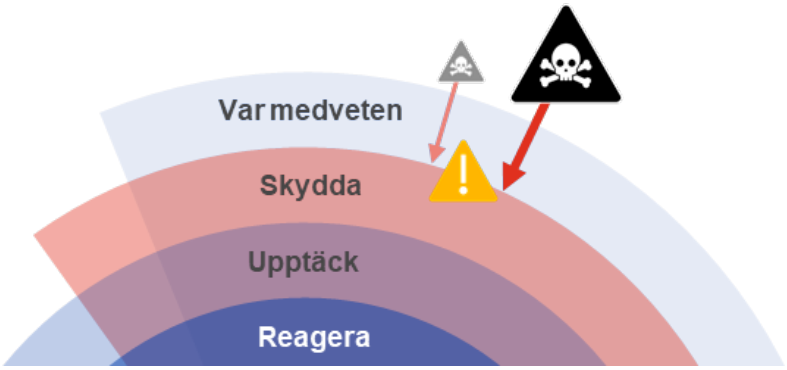

Bild 4: En del angrepp stoppas tack vare skyddsåtgärder

I det här skedet borde er organisation ha en uttömmande lista över all IT-egendom som används (se punkt 3.1), så att åtgärder kan vidtas för att skydda dem. Fokus för skyddsåtgärderna ska i första hand ligga på de tjänster eller system som ni identifierat som mest livsviktiga för er verksamhet.

Er organisations administrativa och tekniska mognadsgrad har stor inverkan på skyddsnivån. Ju större cybermognad er organisation har, desto bättre skydd har den även mot angrepp med utpressningsprogram.

Följande frågor hjälper er att fastställa er organisations tekniska mognadsgrad. Ni kan även komplettera bedömningen av mognadsgraden genom att använda Cybersäkerhetscentrets Cybermätare (https://www.kyberturvallisuuskeskus.fi/sv/vara-tjanster/lagesbild-och-natverksledarskap/cybermataren).

Gå noggrant igenom frågorna nedan tillsammans med era experter:[8] [9]

- Har ni säkerställt att ni har en fungerande kommunikationskanal om ett cyberangrepp skulle inträffa?
- Installerar ni regelbundet och tillräckligt ofta informationssäkerhets- och programvaruuppdateringar? Hur försäkrar ni er om att ni använder endast säkra programversioner?
- Använder ni tvåfaktorsautentisering i alla era tjänster som är öppna för internet?
- Har era system och tjänster testats i fråga om deras informationssäkerhet samt de observationer som gjorts på basis av testningen åtgärdats?
- Är er organisations nätverk på lämpligt sätt skyddat med brandväggar och enheterna skyddade med programvaror för att upptäcka och förebygga angrepp? Använder ni även antivirusprogram och arbetsstationsspecifika brandväggar?
- Har de anställda endast de användarrättigheter och -behörigheter till olika system och tjänster som de behöver i sitt dagliga arbete?
- Använder ni era arbetsstationer endast med behörigheter på användarnivå? Administratörsrättigheter ökar avsevärt angriparens möjligheter att ta sig vidare i ett system.
- Är er organisations datanät indelat i olika delar beroende på användningsändamål? Effektiv segmentering bromsar spridningen av ett angrepp till datanätets olika delar och därmed även till systemen i det.
- Sparar ni nätverks-, system- och tjänstespecifika händelseloggar och hur länge lagras de? Överensstämmer er logghantering med regelverket?

4.3 Upptäck

Även de bästa möjliga skydden kan ibland brista. Därför borde er organisations tjänster, system och nätverk kontinuerligt övervakas för att eventuella angrepp ska kunna upptäckas. Effektiv detektering gör det möjligt att reagera snabbt om skydden enligt punkt 4.2 brister. Ju snabbare ett angrepp upptäcks, desto bättre går det att minska och förhindra skadorna det orsakar.

Er organisations ICT-egendom kan övervakas med hjälp av olika sensorer och säkerhetsprogram. Till stöd för övervakningen kan ni även anlita exempelvis ett säkerhetsoperationscenter, som kan ansvara för övervakningen av hela organisationsnätverket och ofta erbjuder service dygnet runt på helger och till exempel under semesterperioder.

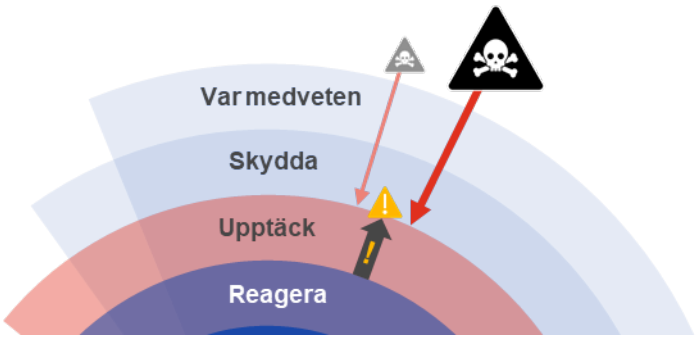

Bild 5: En del angrepp kan tränga igenom skyddsskikten. I sådana fall behövs effektiv detektering, så att er organisation kan reagera på angreppet.

[8] Centre for cyber security Belgium, Incident management guide, https://www.cybersecuritycoalition.be/content/uploads/cybersecurity-incident-management-guide-EN.pdf

[9] CIS, 7 steps to help prevent & limit the impact of ransomware, 2022, https://www.cisecurity.org/insights/blog/7-steps-to-help-prevent-limit-the-impact-of-ransomware

Även medvetenheten hos er organisations personal om risken för angrepp är viktig. Se till att det inom er organisation regelbundet ordnas utbildningar, där man presenterar olika hot och mekanismerna för att de ska realiseras (se punkt 1.2), lär ut rätt förfaringssätt och god cyberhygien samt går igenom vilka åtgärder som krävs vid ett angrepp. Det vore bra för alla anställda inom organisationen att veta hur de ska göra för att agera säkert i sitt dagliga arbete och genom det minska sannolikheten för eventuella angrepp.

Organisationens förmåga att upptäcka angrepp kan även utvecklas och säkerställas med hjälp av olika tekniska bedömningar och testningar. Ett av de bästa sätten att göra detta är genom testning, där utsedda informationssäkerhetsexperter ”angriper” olika delar av datanätet, olika system eller tjänster och representanter för organisationen och dess servicepartner samtidigt försöker upptäcka angreppets olika skeden. Förmågan att upptäcka angrepp preciseras om man inte lyckas upptäcka angreppet, vilket ökar de tekniska kontrollernas effektivitet eller höjer informationssäkerhetspersonalens kompetensnivå.

4.4 Reagera

Utöver effektiv detektering måste man reagera på lämpligt sätt på hot. En observation som ett säkerhetsoperationscenter eller ett program för att upptäcka och reagera på angrepp gör är inte till någon större nytta om er organisation inte vet hur den ska vidta nödvändiga åtgärder. Reaktionerna bör även alltid anpassas efter det upptäckta hotets allvarlighetsgrad, så att man inte stör affärsverksamheten i onödan eller underskattar ett kritiskt hot.

Se till att planer för att hantera informationssäkerhetsavvikelser upprättas för er organisation och att utpressningsprogram tas med i dem som ett möjligt scenario. Försäkra er om att dessa planer är tillgängliga även i offline-version, till exempel i pappersformat. På så sätt finns de till hands, även om ett utpressningsprogram skulle ha krypterat alla era digitala filer.

Fastställ genom avtal och krav vilket ansvar serviceproducenterna har i fråga om att reagera på hot, eftersom en del skadeprogram kan sprida sig även via tredje parter.

Avtala om stödåtgärderna vid tekniska avvikelser med era serviceproducenter, till exempel om den tekniska utredningen och åtgärderna för att minska skadorna. Inkludera dessa i beredskapsplanerna.

Ta även reda på om er organisation behöver en cyberförsäkring och, om ni beslutar er för att skaffa en sådan, se till att de eventuella tjänstekomponenterna i den även inkluderas i återhämtningsplanerna. Kom ihåg att cyberförsäkringen ska vara en väl bevarad hemlighet! Att offentliggöra informationen gör er organisation till ett potentiellt föremål för angrepp.

Se till att era planer regelbundet gås igenom i form av övningar och att de utvecklas utifrån de data, den respons och de tekniska parametrar som ni får genom övningarna. Alla parter som är inkluderade i planerna borde även förstå sin egen roll och kunna agera enligt den vid ett angrepp.

4.5 Återställ

Ibland lyckas angrepp med utpressningsprogram trots beredskapsåtgärder. Det kan finnas olika orsaker till detta, till exempel att något av beredskapsskikten är bristfälligt, att det finns brister i de tekniska kontrollerna eller att en så kallad nolldagssårbarhet har missbrukats (en sårbarhet i en programvara som det inte finns någon korrigerande åtgärd för).

Det är i allmänhet möjligt att återhämta sig från ett storskaligt angrepp med utpressningsprogram om den organisation som utsatts för angreppet har uppdaterade och tillräckligt omfattande säkerhetskopior. I vissa fall, där även säkerhetskopiorna har kontaminerats, behövs dessutom skyddskopior.

För att återhämtningen ska vara effektiv är det skäl att i beredskapen ägna uppmärksamhet även åt den tekniska arkitekturen och förmågan som behövs. Till dessa hör bland annat:

- En säker lagringsmiljö, där den sparade informationens integritet och sekretessgrad säkerställs.
- Logghantering som syftar till att göra det möjligt att följa upp så att säkerhetskopieringen är aktuell och ändamålsenlig.
- Om er organisation använder till exempel virtuella servrar, se till att även de omfattas av säkerhetskopieringen.
- Testning av att återställa säkerhetskopior och säkerställande av att de fungerar.
- En isolerad säkerhetskopieringsmiljö, som förhindrar att säkerhetskopiorna manipuleras eller förstörs.

I punkt 4.1 (Var medveten) ska organisationerna identifiera vilka system och tjänster som är centrala för deras verksamhet. När dessa har identifierats ska tjänste- och systemspecifika återhämtningsplaner upprättas för dem. Syftet med återhämtningsplaneringen är att upprätthålla nödvändig dokumentation, en verksamhetsmodell och en förmåga med hjälp av vilka det är möjligt att återställa tjänsterna eller systemen på ett effektivt och säkert sätt. Återhämtningsplanerna ska förvaras så att de är tillgängliga även om filsystemen inte är det. Det går till exempel att göra papperskopior av planerna.

Annat att tänka på vid återhämtningen och planeringen av den är bland annat:

- I vilken ordning ska systemen återställas? Om systemen återställs i fel ordning kan det orsaka problem eller göra processen att återställa alla kritiska tjänster i sin helhet långsammare.
- Har återhämtningsprocesserna jämte anvisningar beaktats när det gäller de tjänster eller system som upprätthålls av serviceproducenter? Har ni övat återhämtningen?
- Hur säkerställer ni att de tjänster och system som återställs är säkra? Om säkerhetskopiornas versioner, till exempel skyddskopiorna, inte är uppdaterade kan programversioner eller konfigurationer som inte är säkra hamna i produktionen via dem.

5 Källor och ytterligare anvisningar

Anvisningar för ledningen

1. **Cybersäkerhetscentret.** Selviytymisopas kiristyshaittaohjelmia vastaan (Överlevnadsguide mot utpressningsprogram). [Online] 2016. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kiristyshaittaohjelmat__teemakooste_07_2016.pdf

2. **Cybersäkerhetscentret.** Pienyritysten kyberturvallisuusopas (Guide för cybersäkerhet i små företag). [Online] 2020. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Pienyritysten_kyberturvallisuusopas_9_2020.pdf

3. **Suomi.fi.** Dataintrång: informera myndigheterna. [Online] 2022. https://www.suomi.fi/guider/dataintrang/akuta-atgarder/informera-myndigheterna

4. **Forbes.** Ransomware 2.0: How malware has evolved and where it's heading. [Online] 2021. https://www.forbes.com/sites/forbestechcouncil/2021/05/20/ransomware-20-how-malware-has-evolved-and-where-its-heading/

5. **NIST.** Getting started with Cybersecurity Risk Management | Ransomware. [Online] 2022. https://csrc.nist.gov/csrc/media/Publications/white-paper/2022/02/24/getting-started-with-cybersecurity-risk-management-ransomware/final/documents/quick-start-guide--ransomware.pdf

6. **NIST.** Cybersecurity Framework. [Online] 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

7. **NIST**. Ransomware Risk Management: A Cybersecurity Framework Profile. [Online] 2022. https://csrc.nist.gov/publications/detail/nistir/8374/final

8. **GDPR.EU.** What are the GDPR fines? [Online] 2022. https://gdpr.eu/fines/

9. **Cybersäkerhetscentret i Australien.** Ransomware emergency response: one page guide. [Online] 2022 https://www.cyber.gov.au/sites/default/files/2021-10/ACSC-ransomware-emergency-response-one-page-guide.pdf

10. **Ransomware.org.** Everything you need to know about ransomware. [Online] 2022. https://ransomware.org/

Anvisningar för ICT-experter

11. **NIST.** Recovering from Ransomware and Other Destructive Events. 2022**.** https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-11.pdf

12. **CIS.** 7 steps to help prevent & limit the impact of ransomware. [Online] 2022. https://www.cisecurity.org/insights/blog/7-steps-to-help-prevent-limit-the-impact-of-ransomware

13. **CISA.** Cyber security evaluation tool with ransomware readiness assessment module. [Online] 2022. https://www.cisa.gov/stopransomware/cyber-security-evaluation-tool-csetr

14. **Europol.** No more ransom. [Online] 2021. https://www.nomoreransom.org/en/index.html

15. **NIST.** Ransomware protection and response. [Online] 2022. https://csrc.nist.gov/projects/ransomware-protection-and-response

16. **Microsoft.** Ransomware and extortion, a collection of resources. [Online] 2022. https://docs.microsoft.com/en-us/security/compass/human-operated-ransomware

17. **CIS.** 7 steps to help prevent & limit the impact of ransomware. [Online] 2022. https://www.cisecurity.org/insights/blog/7-steps-to-help-prevent-limit-the-impact-of-ransomware

18. **CISA.** Cyber security evaluation tool with ransomware readiness assessment module. [Online] 2022. https://www.cisa.gov/stopransomware/cyber-security-evaluation-tool-csetr

19. **Europol.** No more ransom. [Online] 2021 https://www.nomoreransom.org/en/index.html

20. **NIST.** Ransomware protection and response. [Online] 2022. https://csrc.nist.gov/projects/ransomware-protection-and-response

21. **Microsoft.** Ransomware and extortion, a collection of resources. [Online] 2022 https://docs.microsoft.com/en-us/security/compass/human-operated-ransomware

22. **Sonicwall.** 2022 Sonicwall cyber threat report. [Online] 2022. https://www.sonicwall.com/medialibrary/en/white-paper/2022-sonicwall-cyber-threat-report.pdf

23. **NCSC-UK.** Mitigating malware and ransomware attacks. [Online] 2021. https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks

24. **NCSC-UK.** Mitigating malware and ransomware attacks. [Online] 2021. https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks

Transport- och kommunikationsverket Traficom
Cybersäkerhetscentret

PB 320, 00059 TRAFICOM
tfn 029 534 5000

kyberturvallisuuskeskus.fi

ISBN 978-952-311-802-7
ISSN 2669-8757

Transport- och kommunikationsverket
Cybersäkerhetscentret