NATIONELLT CYBERSÄKERHETSCENTER

Utpressningsangrepp

Temafördjupning

Drabbad av ett angrepp? Agera snabbt och anmäl

Vid en cybersäkerhetsrelaterad incident är det viktigt att skyndsamt vidta rätt åtgärder för att kunna begränsa och bedöma eventuell skada.

- ☑ Vid en cybersäkerhetsrelaterad incident är det viktigt att anmäla händelsen till myndigheter som Polismyndigheten, MSB och IMY, eller andra instanser som är relevanta för verksamheten eller incidenten. Både misstänkta, bekräftade och avslutade incidenter kan vara aktuella att rapportera.
- ☑ Sätt samman en incidentgrupp med tydliga roller. Ta hjälp av externa rådgivare och experter om kompetensen eller tillgängliga resurser inte finns internt. Planera för en långvarig incident, där personal som engageras i ett tidigt skede kan roteras ut efter en tid.
- ☑ Betala inte eventuella krav på lösensumma efter ett utpressnings-angrepp. Det finns inga garantier för att den beslagtagna informationen görs tillgänglig och dekrypteras.
- ☑ Tänk igenom kommunikationsbehoven. Vilka behöver nås av information, när och hur ofta? Utse en person som ansvarar för informationsdelning och vid behov en talesperson. Kommunicera tidigt, tydligt och endast fakta — detta motverkar spekulationer som kan störa incidenthanteringen.
- ☑ För snabbt stöd och vägledning i incidenthantering, kontakta CERT-SE, Sveriges nationella funktion för it-säkerhetsrelaterade incidenter. Kontakta CERT-SE på 010-240 40 40 eller cert@cert.se

NATIONELLT CYBERSÄKERHETSCENTER

Innehåll

Inledning

Utpressningsangrepp har de senaste åren blivit allt mer uppmärksammade, både i samhället och media, på grund av de konsekvenser som de kan orsaka för organisationer och dess intressenter. Förutom att data görs otillgänglig, kan verksamheter även behöva stänga ned system för att utreda och begränsa eventuell skada. Detta kan få ytterligare inverkan på verksamhetens tillgänglighet, information och leveranser. Dessutom finns risken för informationsläckage av känsliga uppgifter. I de fall organisationer inte har en fungerande kontinuitetsplanering på plats, riskerar störningarna att bli allvarligare och framförallt mer långlivade.

Den senaste tiden har det förekommit flera uppmärksammade angrepp där hotaktörer i intrångsfasen har utnyttjat tekniska sårbarheter i kombination med andra sårbarheter i verksamhetens it-miljö. Detta bedöms förbli ett vanligt förekommande tillvägagångssätt.

Det är därför av yttersta vikt att svenska verksamheter, både i privat och offentlig sektor, vidtar säkerhetsåtgärder som försvårar eller avskräcker utpressningsangrepp samt minskar konsekvenserna för lyckade angrepp. Dessa åtgärder spänner över alla aspekter av informations- och cybersäkerhetsarbetet, från ökad säkerhetsmedvetenhet till tekniska administrativa säkerhetsåtgärder.

Rättsvårdande myndigheter världen över har sedan en tid ett ökat fokus på utpressningsangrepp. För att minska konsekvenserna av utpressningsangrepp samt hotaktörernas incitament att genomföra utpressningsangrepp, arbetas nu intensivt med att ta fram och tillhandahålla dekrypteringsnycklar till de organisationer som har drabbats.

Syftet med den här publikationen är att öka medvetenheten kring cyber säkerhetsrelaterade hot, risker och möjliga skyddsåtgärder. Innehållet riktar sig till verksamhetsutövare inom cybersäkerhetsområdet, både inom privat och offentlig sektor.

Publikationen har tagits fram av myndigheterna som ingår i Nationellt cybersäkerhetscenter.

Utpressningsangrepp

I takt med att samhället digitaliserats har även kriminaliteten flyttat in i den digitala sfären. Det går trender i vad som ger god utdelning för de hotaktörer som vill tjäna maximalt med pengar på sin kriminalitet. De senaste åren har utpressningsangrepp blivit en populär inkomstkälla.

Utpressning via gisslantagande är inget nytt fenomen. Opportunistiska aktörer har ägnat sig åt olika typer av gisslantagande och utpressning långt innan samhället digitaliserades. Det digitala gisslantagandet av information skiljer sig dock från de traditionella metoderna, då digitala angrepp kräver en förhållandevis låg insats från hotaktören, med potentiellt hög avkastning i och med det stora antalet möjliga drabbade.

Om en organisations information krypteras, görs otillgänglig eller stjäls, kan den drabbade verksamheten pressas till att betala en lösensumma. Cyberangrepp med element av utpressning har fått en allt större plats i den offentliga debatten, inte minst för att de tenderar att leda till märkbara störningar hos drabbade organisationer, ibland även till den grad att det påverkar externa målgrupper.

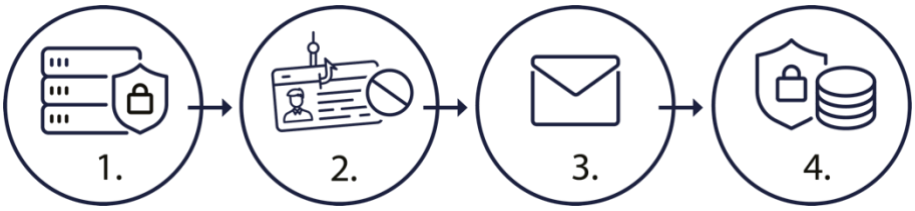
Utpressningsangrepp (eng. *ransomware*) inkluderar hot om att känslig information, exempel personuppgifter, förloras eller riskeras att exponeras. Detta kan leda till allvarliga konsekvenser för verksamheter, individer, men även för samhället i stort. Trots att fenomenet utpressningsangrepp och utpressningsprogramvara blir allt mer känt och rapporterat om i media, bedöms det finnas ett mörkertal i inrapporteringen av dessa angrepp till ansvariga myndigheter.

Utpressningsangrepp som fenomen

Utpressningsangrepp är en typ av cyberangrepp där information beslagtas och görs otillgänglig för verksamheten som drabbas. Det kan få betydande konsekvenser som störningar i verksamhetsutövning, följdeffekter för medborgare eller kunder samt kostnader för hantering och begränsning av eventuell skada. Vanligtvis ställs krav på den drabbade verksamheten att betala en lösensumma för att få tillbaka tillgången till den förlorade informationen. Ibland sker även så kallad exfiltrering, det vill säga att informationen kopieras till en extern plats som hotaktören kontrollerar. I sådana fall kan hot om att offentliggöra information förekomma.

Olika former av utpressningsangrepp

Utpressningsangrepp kan genomföras på olika sätt. En allt mer vanligt förekommande metod är Ransomware as a Service (RaaS), vilket innebär att hela angreppet genomförs på beställning. Beställaren köper i detta fall en metod (1) och väljer sedan själv offer och lösensumma (2). Beställaren sköter också kontakten med offret (3) och delar eventuella lösensummor till aktören bakom RaaS-tjänsten (4).



Så går ett cyberangrepp med Ransomware as a Service till.

I den verksamhet som en hotaktör genomför ingår att kartlägga och planera intrång mot möjliga mål. Det varierar hur långsiktigt och fokuserat arbetet bedrivs. Vissa är opportunister och angriper kända sårbarheter medan andra är mer långsiktiga och aktivt söker sårbarheter hos på förhand utvalda mål. Därutöver finns det ett ekosystem för kriminella där man köpslår om tillgång till utsatta organisationers it-miljöer. De som säljer sådan tillgång kallas Initial Access Broker (IAB). Tillgång till en utsatt organisations it-miljö kan nyttjas på olika sätt beroende på drivkraften hos antagonisten.

Utpressningsangrepp i digitala leveranskedjor

Det digitala samhället medför ofta beroenden mellan organistioner, vilket innebär att även den mest förberedda verksamheten kan falla offer för cyberangrepp. Samtliga verksamheter är på ett eller annat sätt en del av det digitala ekosystemet, vilket innebär att incidenter som inträffar i miljöer som är utom den egna organisationens kontroll kan få stora negativa konsekvenser för den egna verksamheten. Detta kan röra sig om allt från otillgängliga system till utebliven leverans av exempelvis el eller kyla som negativt påverkar förmågan att tillhandahålla en viss tjänst. Dessa händelser är svåra att helt skydda sig mot då alla verksamheter är beroende av leverantörer av olika tjänster och system. Det är dock viktigt att ha en god bild av vilka den egna verksamhetens beroenden är, samt hur dessa kan göras så robusta som möjligt.

It-incidenter som uppstår i digitala leveranskedjor och försörjningsberoenden i it-stöd till samhällsviktig verksamhet bedöms vara den typ av it-incidenter som kan leda till mest omfattande samhällspåverkan. Särskilt när många organisationer använder sig av samma it-leverantör, som hände i fallet med Tietoevry i januari 2024.

Exempel från verkligheten

Utpressningsangreppet som riktades mot Tietoevry den 19 januari 2024 resulterade i att ett stort antal organisationer förlorade tillgången till informationssystem som tillhandahålls av företaget. Bland annat påverkades ett större antal statliga myndigheter men även kommuner, företag och aktörer inom hälso- och sjukvårdssektorn. Omfattningen av störningen varierade från organisation till organisation och berodde ytterst på vilken typ av tjänst som organisationen köpte av Tietoevry och som följaktligen driftades inom den påverkade delen av deras it-miljö.

För de flesta statliga myndigheter som drabbades bestod konsekvensen i att de förlorade tillgången till ett administrativt system som bland annat används för lönehantering och schemaläggning. Det gjorde att de behövde övergå till alternativa rutiner för att exempelvis registerara frånvaro bland personal. I den mån integrationer fanns till andra system påverkades i vissa fall även andra, primärt administrativa, funktioner.

Dessutom påverkades ett flertal aktörer inom hälso- och sjukvårdssektorn. Ett större antal organisationer förlorade tillgången till en tjänst som inom flera regioner används för planering och kommunikation mellan olika vårdinstanser. Det gjorde att flera vårdgivare fick övergå till manuella rutiner för bland annat utskrivning av patienter, exempelvis genom kontakt via telefon. Ett mindre antal aktörer rapporterade även en störning till följd av att ordersystemet tillhörande en leverantör av sjukvårdsartiklar blev otillgängligt. För de allra flesta drabbade aktörerna var tillgänglighets-störningen temporär och informationssystemen återfick funktionalitet i takt med att Tietoevry återställde sin it-miljö, något som i vissa fall tog flera veckor. I ett mindre antal fall gick dock informationstillgångar förlorade.

Motiv, attribuering och hotaktörer

Motiv

Utpressningsangrepp kan vara en finansiellt lönsam modell för att med låg, eller ingen, risk angripa och pressa organisationer på pengar. I takt med den ökande digitaliseringen av it-miljöer blir tillgången till system och information omöjlig att klara sig utan. Bortfall av dessa innebär stora förluster och ibland fara för liv och hälsa. Det ökar pressen på drabbade verksamheter att överväga att betala hotaktören. Motiven till utpressningsangrepp är ofta finansiellt motiverade men andra drivkrafter förekommer.

Attribuering

För att kunna identifiera och tillskriva en aktör bakom ett utpressningsangrepp krävs resurser och tålamod. I vissa fall lämnar hotaktören tydliga spår i form av ett utpressningsmeddelande eller andra kännetecken för att markera att just den grupperingen genomfört ett angrepp, samt för att genomföra eventuella betalningar. I andra fall tar hotaktörer på sig olika angrepp för att skapa uppmärksamhet kring angreppet i sig, eller grupperingen. Dessa uttalanden sker regelbundet och tillförlitligheten i uttalandena är generellt låg.

Grunderna för att kunna identifiera en specifik grupp kallas attribuering och kännetecknas av målval, tillvägagångssätt, tidsperspektiv eller tekniska indikatorer. Detta leder sammantaget till en bedömning av vilken individ, grupp eller organisation som står bakom ett angrepp. Att attribuera till en statlig aktör är svårt och kräver att kopplingen är så pass tydlig att det är meningsfullt att uttala sig om huruvida en statsaktör ligger bakom den kriminella grupperingens handlingar. Ibland krävs omfattande samarbete mellan myndigheter och ibland även stater för att på ett relevant sätt attribuera angreppet.

Dessa utredningar är komplexa och tar mycket tid i anspråk. Vid ett angrepp med utpressningsvirus är det ofta ointressant för den drabbade verksamheten om angreppet orkestrerats av en statlig hotaktör. I de flesta fall går det inte att identifiera en tydlig koppling mellan en kriminell gruppering och en statsaktör. Detta är viktigt att beakta då olika statsaktörer pekas ut i media i samband med uppmärksammade incidenter, ofta på bristfälliga grunder.

Vid attribuering av cyberangrepp är det viktigt att klargöra vilket syfte en eventuell attribuering ska fylla. I brottsutredande syfte kan det vara viktigt att identifiera en gruppering för att kunna lagföra brottet, även om chanserna att väcka åtal och uppnå fällande domar är små. I andra fall kan det vara direkt kontraproduktivt att namnge vissa aktörer och deras eventuella kopplingar, särskilt då de kan vara del av ett större sammanhang där det finns ett intresse av att ostört kunna observera och utreda gruppen eller grupperna.

Olika hotaktörer

Det är viktigt att poängtera att det är flera olika hotaktörer som ägnar sig åt utpressning och beroende på vem det är som står bakom ett angrepp, ser hotet olika ut. I vissa fall är det en hotaktör som utför angreppet, men där en eller flera andra verkar i bakgrunden för att ta del av exfiltrerad data eller annan underrättelse.

Cyberkriminella grupper

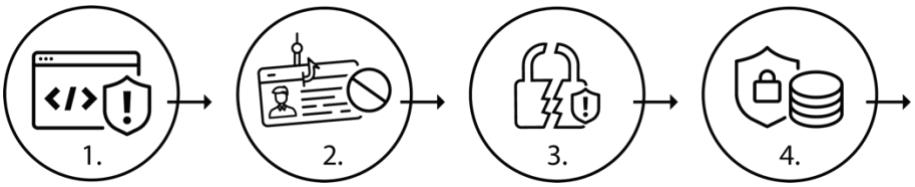
Kriminella grupperingar genomför cyberangrepp som är finansiellt motiverade. Generellt är tillvägagångssätten mindre komplexa och behovet av anonymisering är mindre. Dessa aktörer finns ofta i länder som gör lite eller inget alls för att förhindra cyberkriminalitet. För att bedöma om grupperingarna bara tolereras eller till och med sanktioneras av statliga entiteter krävs mer information än den som kan inhämtas vid utredning av enskilda incidenter. Det man kan göra är att uppskatta sannolikheten.

Statliga aktörer

Statliga aktörer agerar i regel i det dolda, genom förnekbara tillvägagångssätt och genom att dölja sina spår efter ett genomfört angrepp. Syftet med angreppen är inhämtning av begärlig information eller positionering för att kunna kontrollera målets it-system. Statliga cyberaktörer styrs oftast av underrättelse- och säkerhetstjänster och tredjeparter som fungerar som täckmantel.

Angreppets olika faser

Beskrivningen nedan redogör för olika faser i ett typiskt utpressningsangrepp.



Så här går ett utpressningsangrepp till.

Fas 1: Planeringsfas

I planeringsfasen sätter hotaktören upp den infrastruktur som behövs och väljer relevant/ändamålsenlig skadlig kod för att kunna utnyttja sårbarheter.

I den här fasen kan det även ingå samarbeten med andra hotaktörer, exempelvis en Initial Access Broker (IAB) för att köpa sig åtkomst till ett system. En IAB specialiserar sig på att infiltrera olika it-system och företagsnätverk. De samarbetar antingen med ransomware-aktörer för en del av vinsten, eller säljer åtkomster till högstbjudande.

Fas 2: Intrångsfas

I intrångsfasen skaffar sig hotaktören obehörig åtkomst till vald it-miljö. Historiskt sett har många utpressningsangrepp påbörjats genom att lura en användare att köra skadlig kod, ofta genom nätfiske (eng. *phishing*). Att sprida skadlig kod eller skadliga länkar via e-post är en vanligt förekommande intrångsvektor i samband med utpressningsangrepp. På senare tid har sårbarheter i exempelvis tjänster för fjärråtkomst (t.ex. vpn) allt oftare använts som intrångsvektor.

Nätfiskekampanjer kan vara mer eller mindre sofistikerade. De kan vara storskaliga angrepp där miljontals bedrägliga meddelanden skickas ut i hopp om att någon ska luras att ladda ned skadlig kod. Det kan dock även handla om riktat nätfiske mot specifika mottagare och verksamheter (eng. *spear phishing*). Hotaktören kan också skanna internet efter sårbara system som kan utnyttjas för att få tillgång till it-miljöer.

Organisationer brister emellanåt i att härda sina it-miljöer. Detta kan exempelvis visa sig genom att sårbara tjänster exponeras mot internet utan lämpligt skydd. Ett system som inte uppdateras är sårbart men trots att system uppdateras kan det finnas sårbarheter i form av nolldagarssårbarheter (eng. *zero-day attack*), som inte upptäckts av leverantören och därmed inte omhändertagits genom en uppdatering. Den vanligaste intrångsvektorn är genom kända sårbarheter.

Fas 3: Exploateringsfas

När hotaktören har tagit sig in i nätverket vidtas åtgärder för att bibehålla närvaron och gräva sig djupare in i it-miljön. Hotaktören kan exempelvis skapa bakdörrar i internetexponerade system, skapa fler användarkonton eller ändra system-konfigurationer för att skapa hemliga åtkomstpunkter. Målet är att säkerställa fortsatt tillgång till it-miljön även om det första intrånget upptäckts och åtgärdats. När hotaktören väl är inne i den drabbade organisationens nätverk är det svårare att upptäcka angreppet. Genom att använda den mjukvara som den drabbade själv har installerat kan hotaktören ta sig runt i nätverket utan att lämna allt för tydliga spår efter sig.

Förutom att oupptäckt kunna röra sig i ett drabbat system, vill hotaktörer ofta skapa sig så stor kontroll som möjligt. Det innebär att de försöker utöka rättigheterna som de initialt tillskansat sig, med ambitionen att öka sin förmåga att kontrollera it-miljön. Hotaktören vill kunna kryptera så mycket data som möjligt och i vissa fall stjäla känslig information. Om det handlar om mycket data kan detta pågå under en längre tid. Hotaktören försöker därför undvika att bli upptäckt. Ofta finns kopplingar till andra it-miljöer och vägen in i ett nätverk kan göra att fler organisationer blir drabbade. Detta är särskilt tydligt i de fall en hotaktör får tillgång till en tjänsteleverantörs it-miljö, som genom sin utformning, möjliggör åtkomst till kunders it-miljö och data.

Fas 4: Utpressningsfas

Den skadliga koden för själva utpressningsviruset installeras som sista steget i ett angrepp. I den här fasen har hotaktören antingen laddat hem all information av intresse, eller så riskerar den att bli upptäckt och avslutar angreppet i förtid. Hotaktören vill också säkerställa att den drabbade organisationen vet vem som angripit dem och framförallt hur de ska betala för att få tillbaka sin information. Med andra ord vill hotaktören säkerställa att den drabbade organisationen hittar deras krav på lösensumma. När utpressningsviruset har aktiverats kan det snabbt kryptera filer och låsa användare ute från system, vilket för många drabbade är den första indikationen på ett utpressningsangrepp. Tiden det tar för fullständig kryptering beror på många faktorer, bland annat vilken skadlig kod som använts, hur stor datamängd som ska krypteras samt nätverkets uppbyggnad. Det kan ta från några timmar upp till dagar. Hotaktörer kräver ofta flera betalningar, där den första kan vara för att dekryptera filer eller system. Efterföljande krav kan vara betalningar för att returnera eller förstöra exfiltrerad information.

Konsekvenser

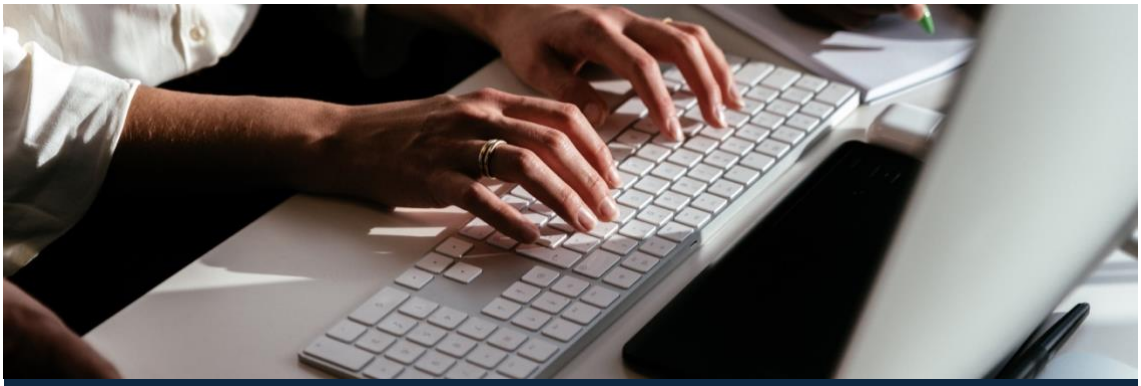
Angrepp med utpressningsprogramvara kan vara lamslående för enskilda verksamheter då it-system helt eller delvis behöver stängas ned för att begränsa och utreda omfattningen av angreppet och eventuell skada. Ofta kan verksamheten fortgå med hjälp av backupsystem och manuella rutiner, men det är olika från fall till fall och beror till stor del på organisationens beredskap och kontinuitetsplanering.

Det är viktigt att inte tillmötesgå eventuella krav på lösensumma efter ett utpressnings-angrepp. Det finns inga garantier att system återställs, att filer dekrypteras, att stulen information raderas eller att hotaktören inte fortsätter att komma med nya krav eller hot. För en organisation utan backuplösningar kan det givetvis vara lockande att betala för att återfå sin information eller systemkonfiguration. Data som på olika sätt exponerats för obehöriga, särskilt i antagonistiskt syfte, är dock bäst att betrakta som förlorad, då man sällan kan bedöma hur informationen kan komma att användas i ett nästa steg.

Allvarlighetsgraden av ett utpressningsangrepp beror på vilken typ av verksamhet som drabbats och om den är samhällsviktig. Försörjningsberoenden mellan it-system är en viktig faktor, då ett utpressningsangrepp hos en organisation kan få konsekvenser för verksamheter långt utanför den drabbade it-miljön.

Vid långvariga störningar i samhällsviktig verksamhet, som till exempel hälso- och sjukvård, kan konsekvenserna av ett utpressningsangrepp bli ytterst märkbara. För mindre kritiska verksamheter kan dock ett utpressningsangrepp, särskilt om de inträffar samtidigt som andra störningar internt eller i omvärlden, ha en stor påverkan på en organisations förmåga att utöva sin kärnverksamhet.

Till följd av ett inträffat angrepp finns flera aspekter att ta hänsyn till, både på kort och längre sikt. Först och främst finns risken för människors liv och hälsa. Om det dessutom skulle inträffa flera parallella händelser i samband med ett utpressningsangrepp finns risken att konsekvenserna förvärras avsevärt. Vidare påverkas ekonomin både på kort och lång sikt hos den drabbade verksamheten. Under återställningsfasen tas ofta externa konsulter i anspråk för hjälp med hantering, vilket kan innebära stora kostnader. Detta får sannolikt konsekvenser för organisationen under lång tid, särskilt om den drabbade organisationen exempelvis är ett litet företag eller mindre kommun. Därtill kan organisationens anseende och/eller varumärke påverkas. Även tilliten från kunder/användare/medborgare kan påverkas negativt av den inträffade incidenten.



Exempel från verkligheten

En organisation inom offentlig sektor drabbades av ett utpressnings-angrepp. Filer på en filserver samt en applikationsserver blev krypterade. Källan till angreppet kunde spåras till en dator som hade anslutit till nätverket, varpå filkryptering hade kunnat pågå i drygt tre timmar. Användaren till den utnyttjade datorn hade märkt av problem med enheten vid arbete i hemmet dagen före angreppet. När datorn startades upp på kontoret öppnades flera terminalfönster på skärmen, med information som användaren inte förstod. Hen tog då kontakt med it-avdelningen för att installera om datorn, vilket medförde att krypteringen av filer på filservern avbröts. Angreppet kunde begränsas relativt fort och en första analys av angreppet visade inga indikationer på sidosteg i it-miljön. Angreppet polisanmäldes.

Som med andra problem eller störningar, bidrar ett proaktivt säkerhetsarbete till att bättre klara av konsekvenserna av ett angrepp. It-säkerhetsrelaterade incidenter – och störningar i allmänhet – kan bli kostsamma för organisationer. Även om det inte hjälper vid den operativa hanteringen av ett utpressningsangrepp, är det betydligt billigare och mer effektivt att arbeta förebyggande för att minimera effekterna av angrepp överlag, och angrepp med utpressningsvirus specifikt.

Gällande konsekvenser är det till stor del förmågan att upprätthålla funktion utan tillgång till data eller system som är avgörande för i vilken utsträckning som verksamheter påverkas. I de fall konsekvenserna blivit allvarliga och omfattande har ofta hela miljöer, inklusive backuper, krypterats och gjorts obrukbara. Detta illustrerar vikten av att hantera säkerhetskopior på ett bra sätt (se rekommendationer på s.17), samt att regelbundet öva återställning och återläsning.

Exempel från verkligheten

En organisation inom privat sektor drabbades av ett utpressningsangrepp. En hotaktör fick tillgång till it-miljön via en vpn-lösning, efter att ha kommit över inloggningsinformation till administratörskontot. Troligtvis kom hotaktörer över inloggningsinformationen genom ett angrepp mot organisationens it-leverantör.

Efter att ha loggat in påbörjade hotaktören Active Directory-synk mot organisationens domänkontrollant. Hotaktörer hade tillgång till it-miljön i ett fåtal minuter innan systemet låstes och internetåtkomsten stängdes ned. Den troliga ingångsvektorn var en tidigare sårbarhet som utnyttjades.

Vidtagna åtgärder till följd av angreppet inkluderade byte av lösenord på alla administratörskonton och servicekonton, införande av multifaktor-autentisering på vpn-tjänster, byte av brandvägg till en produkt med bättre larmfunktioner vid inloggning på vissa konton, samt bättre verktyg för logghantering. Angreppet är polisanmält.

Ytterligare en möjlig konsekvens är att stora mängder information som röjts i och med ett angrepp kan nyttjas av hotaktörer. Att komma över och sedan sälja känslig information är ytterligare ett sätt för cyberkriminella att tjäna pengar. När en kriminell aktör kommit över data som sedan säljs till högstbjudande, innebär det ett scenario som skulle kunna ge statliga aktörer tillgång till stora mängder känslig information. Denna information kan, om den sammantaget ger information om sakernas tillstånd i Sverige, vara information som är att betrakta som säkerhetsklassificerad information.

Att förebygga och hantera utpressningsangrepp

Det är svårt att helt undvika olika typer av störningar och cyberangrepp i digitala miljöer. Det finns dock mycket organisationer kan göra för att stärka sin motståndskraft och förmåga att förebygga och hantera cyberangrepp i allmänhet, och utpressnings-angrepp i synnerhet. Att aktivt och regelbundet arbeta med sitt tekniska skydd räcker långt, men det är viktigt att även lägga resurser på beredskaps- och kontinuitetsarbete samt att bygga en säkerhetsmedveten arbetskultur. Till dessa insatser hör också att öva och utbilda sina medarbetare, både för att förhindra och bättre kunna hantera ett cyberangrepp. Om medarbetare vet vad de ska göra om it-miljön drabbas av störningar, kan lugn och fokus bevaras. En viktig del i att skapa en effektiv säkerhetskultur är att främja en tillåtande arbetsmiljö där medarbetare uppmuntras att rapportera säkerhetsrelaterade incidenter och avvikelser, utan oro för eventuella konsekvenser eller känslan av att ha begått ett misstag.

Till skillnad mot vad många tror, förutsätter utpressningsangrepp sällan sofistikerade metoder eller av hotaktören väl uttänkta, riktade angrepp. Ofta sker intrång och exekvering av utpressningsprogramvara till följd av att hotaktören hittat sårbara system och/eller brister i den grundläggande cyberhygienen hos en organisation. Organisationer kan alltså komma en god bit på vägen i att minska sin sårbarhet för angrepp genom att införa grundläggande säkerhetsåtgärder.

En framgångsfaktor som allt oftare framhålls, är vikten av att känna sin it-miljö – både tekniska lösningar, användare och eventuella beroenden i digitala leverans- eller försörjningskedjor. Känner man sin it-miljö, och har stöd av tekniska lösningar, blir det lättare att upptäcka avvikelser och därmed kunna hantera och begränsa olika typer av störningar. Tidig upptäckt och en tydlig incidenthanteringsplan möjliggörs av både ett kontinuerligt och systematiskt säkerhetsarbete.

När det gäller antagonistiska angrepp är det viktigt att i så hög grad som möjligt försvåra för hotaktören, och göra it-miljön oattraktiv att angripa. En organisation med ett genomtänkt tekniskt skydd och hög säkerhetsmedvetenhet bland medarbetare, blir per automatik en mindre intressant måltavla för cyberkriminella. Har organisationen därtill en genomtänkt strategi för backuper och beredskap, ökar möjligheten att klara ett angrepp utan större påverkan på verksamheten.

Arbeta aktivt med ett gott tekniskt skydd

Att medvetet bygga, anpassa och underhålla ett gott tekniskt säkerhetsskydd är en förutsättning för att kunna stoppa och hantera cyberangrepp. På samma sätt är det avgörande för hur väl en organisation lyckas parera eller minska konsekvenserna av just utpressningsangrepp.

Många system som används i en verksamhets it-miljö har säkerhetsfunktioner inbyggda. Utöver detta finns specialiserad teknisk utrustning som kan integreras i miljön för att utöka dessa säkerhetsfunktioner. Exakt vilka sådana funktioner som är lämpliga för en given verksamhet utifrån hotet från utpressningsangrepp, behöver baseras på en riskanalys av verksamhetens informationshantering. Det finns dock mycket att göra genom att inventera sina nuvarande lösningar och aktivera redan befintliga funktioner. Som ett komplement kan organisationer även anmäla intresse för CERT-SE:s funktion ANTS, automatiska notifieringar för tekniska sårbarheter. Det är automatiserade utskick där organisationer uppmärksammas om tekniska företeelser som kan behöva åtgärdas i deras it-miljö.

Tips och råd

För att försvåra för en hotaktör måste verksamheten kontinuerligt bedriva ett systematiskt informations- och cybersäkerhetsarbete. Denna sammanställning av rekommenderade säkerhetsåtgärder utgör ett stöd i arbetet med att prioritera vad som behöver göras om ett angrepp inträffar. I det systematiska säkerhetsarbetet ingår även administrativ säkerhet samt att aktivt bygga en säkerhetskultur.

1. **Installera säkerhetsuppdateringar så fort det går**

Prioritera att uppdatera informationssystem som exponeras mot internet, de som är verksamhetskritiska och de där sårbarheter riskerar att utnyttjas. Ha som målsättning att installera säkerhetsuppdateringar snarast efter att de publicerats.

2. **Förvalta behörigheter och använd starka autentiseringsfunktioner**

Ha kontroll på alla konton i it-miljön, inaktivera de som inte används. Var strikt med de behörigheter som är tilldelade. Använd multifaktorautentisering på alla publikt exponerade tjänster, för åtkomst till information med högt värde och för konton med systemadministrativa behörigheter. Där multifaktorautentisering inte stöds, använda unika och långa lösenord.

3. **Begränsa och skydda användningen av systemadministrativa behörigheter**

Använd separata konton för systemadministrativa behörigheter. Avgränsa även behörigheter till uppgifter, roller och delar av it-miljön. Tilldela inte vanliga användare systemadministrativa behörigheter.

4. **Inaktivera oanvända tjänster och protokoll (härda systemen)**

Säkerställ att funktioner som inte behövs för önskvärd funktionalitet i informationssystemen stängs av, blockeras eller avinstalleras. Konfigurera informationssystemen att ha en hög säkerhet.

5. **Gör säkerhetskopior och testa att informationen går att läsa tillbaka**

Skapa säkerhetskopior på information utifrån verksamhetens behov. Hantera säkerhetskopiorna säkert och testa periodiskt att det går att återställa informationen på dem.

6. **Tillåt endast godkänd utrustning i nätverket**

Endast tillåten utrustning ska kopplas till nätverket. Otillåten utrustning behöver upptäckas och dess åtkomst till tjänster och information i it-miljön förhindras.

7. **Säkerställ att endast godkänd mjukvara får köras (vitlistning)**

Förhindra att otillåten mjukvara körs i it-miljön.

8. **Segmentera nätverken och filtrera trafiken mellan dem**

Upprätta olika nätverkssegment och skapa kontrollerade trafikflöden mellan dem med hjälp av filtreringsfunktioner som skyddar mot att oönskad trafik kan flöda fritt i nätverket.

9. **Uppgradera mjuk- och hårdvara**

Byt ut och ersätt föråldrad hård- och mjukvara för att motverka sårbarheter som över tiden exponerats och för att få avsedd funktion och tillräcklig säkerhet.

10. **Säkerställ förmågan att upptäcka säkerhetshändelser**

Skaffa förmågan att upptäcka säkerhets-händelser i it-miljön så tidigt som möjligt. Övervaka händelser i it-miljön med manuella, tekniska och automatiska åtgärder. Skapa säkerhetsloggar som kan användas för övervakning och som skyddas mot obehörig åtkomst eller förändring.