Hackerattacken som sänkte detaljhandeln

- Ett whitepaper om hur rapid response och recovery vände krisen – och hur din organisation kan skydda sig

Cyberattacker är ett växande globalt problem, och en typ av kriminalitet som blir allt mer allvarlig i ett samhälle som fortsätter att digitaliseras i rasande fart. Attackerna har varierande allvarlighetsgrad: vissa skapar merarbete för it-avdelningen medan andra kan lamslå hela organisationen och förstöra stora ekonomiska värden.

Internationella säkerhetsexperter har länge varnat för att det bara är en tidsfråga innan en cyberattack orsakar omfattande skada på samhället. I Sverige har SÄPO varnat för att främmande makt utgör ett allt allvarligare hot mot svenska företag och offentliga organisationer, medan MSB vid flera tillfällen varnat för att man ser att ökande antal såkallande ransomwarekampanjer som riktar sig mot Sverige: attacker där angriparna gör intrång i en verksamhets it-system och krypterar information för att få de drabbade att betala en lösensumma.

I juli 2021 inträffade precis en sådan attack. Den drabbade den amerikanska mjukvaru-leverantören Kaseya, och i förlängningen ett stort antal av deras kunder som använde deras klienter – bland annat flera svenska butikskedjor med hundratals butiker.

I detta whitepaper ska vi se närmare på världens hittills största ransomwareattack, hur den påverkade svensk detaljhandel – och hur Visma EssCom och våra partners arbetade med att lösa krisen.

När verksamheten avstannar

På fredagskvällen går larmen. Först från en stor butikskedja: En prio 1-incident har ägt rum, kassorna fungerar inte. Prio 1-incidenter inträffar någon gång per år, de tas alltid på allvar men behöver inte nödvändigtvis vara så komplicerade att lösa. Men någon minut senare kommer ett nytt larm, denna gång i form av en malwarevarning från Vismas AI-baserade intrångsdetektion. Därefter ett till larm från Kaseya självt, med uppmaning om att ta ner samtliga installationer omedelbart. 90 sekunder senare är samtliga servrar frånkopplade, och en lång natt av skadeutvärdering inleds.

Just nu är prioriteten att säkra systemen och skademinimera. Är det ett pågående angrepp, eller stoppades det av att servrarna kopplades ner? Två timmar efter attacken är TrueSec på plats och påbörjar det forensiska arbetet. Den forensiska analysen kommer senare att upptäcka flera allvarliga sårbarheter i Kaseyas system, några totalt oacceptabla. Men i denna stund vet ännu ingen hur allvarlig attacken är, eller vilket jobb som kommer att krävas för att återställa alla system.

På lördagsmorgonen står det klart att attacken är av aldrig tidigare skådad omfattning, och att tusentals klienter kommer att behöva återställas. Olika kunder använder olika system, och via olika temporära lösningar kan två butikskedjor börja ta betalt. Nu har även NOA hört av sig, Polisens Nationella Operativa Avdelning. Polisen har insett attackens omfattning och vill skapa sig en bild av samhällspåverkan och om skadorna överhuvudtaget kommer gå att reparera.

> Vi hade massor av idéer på hur vi skulle komma runt problemen, men det var enormt svårt att hitta något som fungerade i stor skala, säger Fabian Mogren.

Logistiska utmaningar

Under söndagen har arbetet börjat bära frukt, och Visma EssCom börjar arbetet med att rulla ut en lösning. Men de logistiska utmaningarna är inte små: en stor andel av butikerna har idag, förutom alla kassor även fysiska servrar, vilket betyder att tekniker behöver skickas ut. Till varje butik.

”Ransomware har exploderat de senaste tre åren. Det är inte bara en ekonomisk förlust, utan skadar också företagets varumärke.” – Mikael Westerlund, Globalconnect.

När verksamheten avstannar

”Vi bröt alla semestrar som gick att bryta och kallade in all tillgänglig personal. Dessa förstärktes med Vismakollegor från Norge. Dessutom dammsög vi marknaden på tekniker med relevant kompetens, berättar Fabian Mogren. Det var enormt hektiska dygn, men det var en stor tillgång att vara en del av Vismakoncernen och ha tillgång till hela den organisationens styrka.

En knapp vecka efter att attacken ägt rum är alla butiker öppna igen. Under den första dygnen har fokus legat stenhårt på att få igång kassorna, så att butikerna vars omsättning sjunkit till noll ska kunna sälja varor igen. Anställda har arbetat i skift, dygnet runt, och utmattningen i personalstyrkan börjar bli påtaglig. Tempot saktas nu ned, och medarbetare som sovit ett par timmar per dygn får möjlighet att återgå till en normal dygnsrytm. Under söndagen, dag 9 efter attacken, övergår arbetet till nästa steg: total återställning och utrensning av skadlig kod. System som körts i begränsat läge kan nu återställas till full funktionalitet, ett arbete som tar ungefär två veckor. Under tiden har NOA överlämnat ärendet till regionalt it-brottscentrum, där själva brotts-utredningen kommer att fortsätta framöver.

Långt efterarbete

När fas 2 stängt är det dags att ta itu med nästa utmaning: att hitta en lämplig väg framåt. – Fas 3 kommer att pågå länge, säger Fabian Mogren. Vi har fått enormt mycket kunskap under arbetets gång som vi nu kan ta med oss i den fortsatta utvecklingen. Flera av kunderna har helt tappat förtroendet för Kaseya, och utmaningen nu blir att hitta en lösning som uppfyller alla krav på funktionalitet och dessutom har tillräcklig säkerhet.

Det finns bara en handfull leverantörer globalt som har lösningar på den nivån, men att implementera en installation på den här skalan är en lång process.

Parallellt med det tekniska arbetet kommer de juridiska dimensionerna av attacken att ta mycket resurser framöver. Alla inblandade aktörer har liabilityklausuler i sina inbördes avtal, klausuler som nu aktiveras i och med att de ekonomiska skadorna ska identifieras och beräknas. Samtidigt påbörjas en rad försäkringsärenden, där ansvarsområden behöver fastställas i detalj. Därtill kommer den rena brotts-utredningen, och ett eventuellt efterspel på politisk nivå.

Hur kunde situationen uppstå?

- **Zero-day vulnerabilities i Kaseyas kod**
- **Eftersatt infrastruktur hos kunderna**
- **Spretig IT-miljö med många olika versioner och operativsystem**

”En av de bredaste, kraftfullaste attacker av en icke-statlig aktör som vi har sett” – Andrew Howard, Kudelski Security

En incident som avslöjade brister

Det är alltid lätt att vara efterklok. Efter en lyckad attack är det förstås alltid möjligt att undersöka de felande länkarna i säkerhetskedjan och se vad som hade kunnat göras annorlunda. För att en incident av den här magnituden ska kunna inträffa måste väl något ha varit allvarligt fel?

– Det är inte så enkelt, förklarar Fabian Mogren. Det går inte att gardera sig mot samtliga tänkbara attacker, allt man kan göra är bygga ett så säkert system som möjligt utifrån den information man har. Innan Kaseyas system installerades hos Visma EssComs kunder gjordes en gedigen utvärdering av såväl mjukvaran som leverantören.

– Det var en hård utvärdering som vi var väldigt stolta över, och faktum är att den håller än! säger Fabian Mogren. Kaseya är ett stort, välrenommerat bolag med alla nödvändiga certifieringar och var dessutom vid tiden för upphandlingen en av få leverantörer med ett prickfritt förflutet. Deras verktyg hade inte hackats förr, det var till och med en del av deras marknadsföring.

Raserat förtroende

Kaseyas verktyg valdes på grund av sin höga accountability och lämplighet för krävande enterprisemiljöer. I incidentens kölvatten har dock besvärande information uppdagats. Det har visat sig att Kaseya inte riktigt levt upp till den uppgivna nivån: Företaget har inte agerat på säkerhetshål som hade rapporterats in långt innan attacken, och inte uppfyllt sina egna certifieringar. I den forensiska analys som Visma EssCom genomförde och som validerades av TrueSec upptäcktes flera sårbarheter som härrörde sig till rent slarv från utvecklarens sida. Det har också kommit fram att Kaseya hade flyttat delar av utvecklingen till Minsk i Ryssland, utan att meddela sina kunder.

– Det spelar ingen roll vilket avtal man har om leverantören aktivt bortser från att följa uppsatta krav, säger Fabian Mogren.

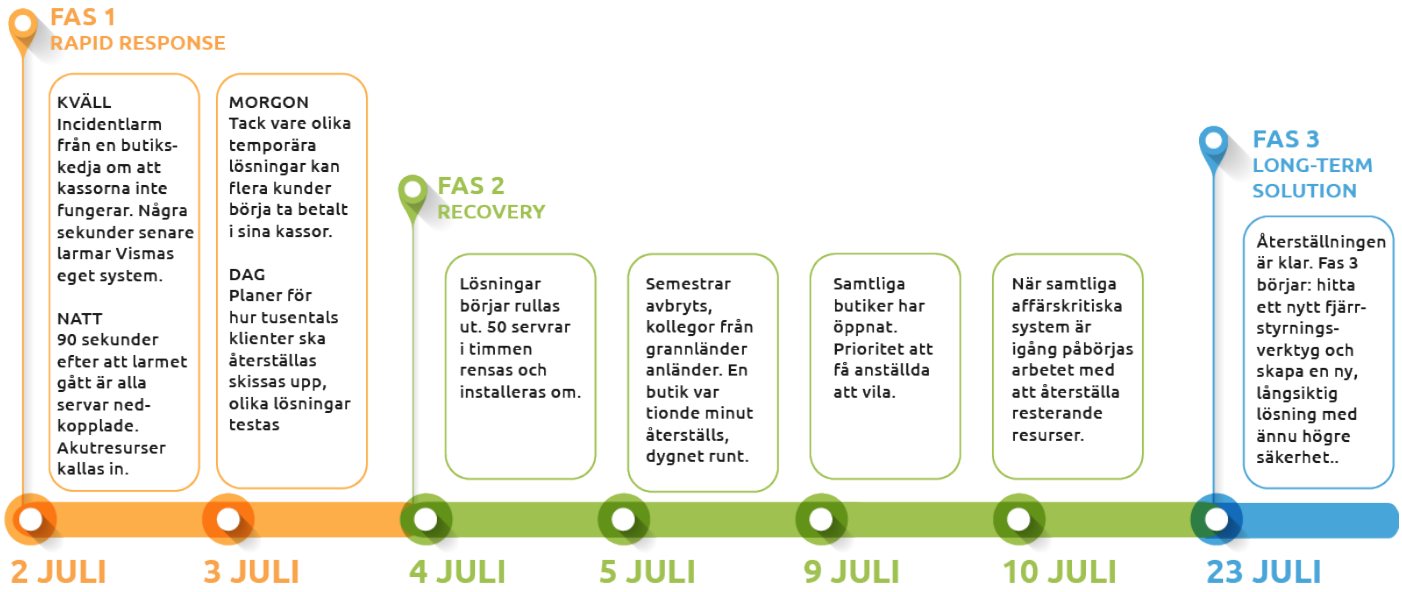
> Vår miljö var uppsatt långt över branschpraxis och Kaseyas specifikation, med AI-driven övervakning och alla möjliga säkerhetsfunktioner – ändå gick det fel. Det tog Kaseya tio dagar att leverera en patch, eftersom de upptäckte nya säkerhetshål under arbetets gång. Det är inte så att man jublar som kund…

Efter attacken har Visma EssCom noggrant utvärderat sina rutiner. Rutiner kan alltid förfinas, men incidenten har blivit en påminnelse om att det inte går att gardera sig till hundra procent så länge man använder sig av underleverantörer. Någon kommer alltid att kunna begå ett misstag, slarva eller skära in på en kostnad på ett oacceptabelt men osynligt sätt som inte uppdagas i tid.

– Har man kritiska system och vill gardera sig så långt det bara är möjligt måste man genomföra egna audits, säger Fabian Mogren. Men det är resurskrävande och även med alla våra processer kommer det inte att lösa allt – någon med uppsåt kommer alltid att kunna orsaka skada. Det är i grunden en allmän risk, och inte en risk som är specifik för it-miljöer.

Att arbeta igenom en kris

TIDSLINJE



Kaseya-incidenten är den största kända ransomware-attacken hittills, men riktade sig inte mot Sverige specifikt. De svenska butikskedjorna hamnade i ett slags internationell korseld, utan att någonsin ha varit det primära målet. Trots att de drabbades hårt var betalning av lösensumman aldrig ett alternativ.

– Att betala de kriminella är det bästa sättet att hålla den här verksamheten lönsam, så det var glädjande att ingen av våra kunder ens övervägde det, säger Fabian Mogren. Men det var också korkat av angriparna att utpressa så att det syntes publikt. Inget företag vill figurera i pressen som den som betalade. Inte ens ur ett rent ekonomiskt perspektiv är betalning en god idé – forskning visar att den totala kostnaden nästan fördubblas för dem som väljer att betala lösensumman. [Källa: Sophos, The State of Ransomware 2020]. Lösensumman blir en enorm utgift som inte minskar tiden för att återställa servrar, inkomstbortfall under nedtiden och andra operationella kostnader påtagligt.

Vikten av en krisplan

När it-säkerhet diskuteras ligger fokus ofta på intrångsskyddet. Men att identifiera och förhindra attacker på servrar och tjänster är bara halva lösningen. Cyberkriminalitet är ett snabbt växande problem och det är bara en tidsfråga innan ett skydd penetreras. Recovery måste därför vara en del av varje företags it-strategi.

> Det är inte frågan om det kommer att hända, utan när, säger Fabian Mogren. Att inte ha en täckande krisplan för allvarliga incidenter är nästintill oansvarigt.

En allvarlig attack kan ha katastrofala konsekvenser för verksamheten, även i de fall samhällspåverkan är begränsad. Kaseya-attacken innebar tusentals butiker över en natt tappade hela sin omsättning, och i initialskedet visste ingen när eller ens om situationen skulle kunna redas ut.

Att arbeta igenom en kris

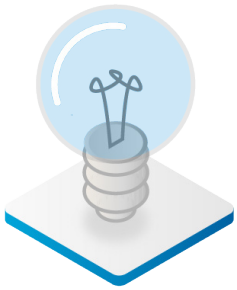
”Intrång är alltid allvarliga, men när de med omedelbar verkan sätter stopp för kundens hela revenue stream är paniken nära, säger Fabian Mogren. Recovery är vår hemmaplan och vi är alltid beredda på brand, men den här gången var det mer som en härdsmälta på ett kärnkraftverk.

Personalen påverkas

Lärdomarna från krisarbetet är många. En något oväntad insikt blev hur starkt krisen påverkade medarbetarna psykologiskt.

– Det allmänna trycket i organisationen ökade på ett obeskrivligt sätt, minns Fabian Mogren. Våra anställda arbetade oerhört hårt i en pressad situation, och det resulterade i att två blev sjukskrivna och många andra mådde dåligt. Tänk dig en situation där kunder vill ha uppdateringar varje timme, polisen ringer, aktieägare är oroliga, koncern-ledningen behöver hållas informerad – under tiden som dagspressen letar efter syndabockar och förmedlar grovt förenklade och felaktiga bilder av vad som händer. Det uppstår slitningar i personalen, som dessutom slits mellan jobb och familj.

En del av en bra krisplan är att vara beredd på hur personalen kommer att reagera. Det kommer att tas fram idéer, men vissa initiativ kommer att vara direkt kontraproduktiva. Att hålla huvudet kallt och ha en tydlig ledarstruktur är nödvändigt för att organisationen ska kunna fungera effektivt i en kaotisk situation. Lika viktiga är rutiner kring arbetstid och fördelning av uppgifter.



Vanliga sårbarheter som angripare utnyttjar

- **Brister i behörighetshantering och autentiseringsmekanismer**
- **Svagheter i it-arkitekturen, exempelvis otillräcklig separering av nät**
- **Bristande underhålls-, livscykel- och updateringsrutiner**
- **Bristande säkerhetsnivå på interna applikationer**
- **Ej administrerad och hanterad utrustning som ansluts till nätverket**
- **Bristfällig loggning och detektion**
- **Aktiva konton för medarbetare som inte längre arbetar kvar**
- **För låg kunskap i organisationen om incidentupptäckt och hantering**
- **Bristande säkerhet hos leverantörer av hård- och mjukvara eller tjänster**

Källa: Cybersäkerhet i Sverige – rapport från Försvarets radio-anstalt, Försvarsmakten, Myndigheten för samhällsskydd och beredskap, Polismyndigheten och Säkerhetspolisen.

Att arbeta igenom en kris

När alla kommer springande och vill hjälpa till är det lätt att det skapas mer kaos, men med bra kommunikation och resursfördelning kan alla arbeta så effektivt som möjligt mot samma mål. Kaseya-attacken har också visat hur viktigt det är att ha tillgång till relevanta resurser i en pressad situation.

– Det borde finnas en överenskommelse i branschen att alla hjälper till när allvarliga attacker inträffar, säger Fabian Mogren. Tänk om vi kunde skapa telefonlistor med nödnummer, även till konkurrenter, där drabbade snabbt kan få tag i hjälp. Den här attacken är avvärjd, men det är bara en tidsfråga innan en ny, stor incident inträffar.

”Ett exempel på vad som i en mer omfattande skala skulle kunna hamna i ett skarpt säkerhetspolitiskt läge” – Peter Hultqvist, försvarsminister

Så går ett angrepp till

- **Den kriminella aktören planerar operationen och väljer ut lämpliga mål utifrån attackens syfte, till exempel ekonomisk utpressning, spionage eller sabotage.**
- **De tilltänkta målen kartläggs: information om t ex it-miljö, rutiner, tillgångar eller anställda kan vara värdefull.**
- **Nu börjar arbetet med att hitta och identifiera sårbarheter, och planer för hur dessa kan utnyttjas mest effektivt.**
- **Cyberattacken påbörjas. Om den lyckas kan angriparna få allt från delvis insyn i, till total kontroll över målets it-miljö.**
- **När angriparna kan agera inne i it-miljön genomförs de olika aktiviteter som var syftet med intrånget, exempelvis stöld av värdefull information eller sabotage av filer.**

Källa: Cybersäkerhet i Sverige – rapport från Försvarets radio-anstalt, Försvarsmakten, Myndigheten för samhällsskydd och beredskap, Polismyndigheten och Säkerhetspolisen.

Vill du veta mer om hur Visma EssCom kan hjälpa din organisation – kontakta oss på 010 - 141 16 00 eller info.esscom@visma.se