Checklista:

Nio sätt att skydda din organisation mot ransomware

GlobalConnect

Cyberbrottslighet är en lönsam verksamhet som omsatte mer än hela den globala droghandeln under 2021. Hur ser hotbilden från ransomwareattacker ut idag, och hur kan du skydda din organisation från intrångens kostsamma effekter? Det får du veta i denna guide, som vi på GlobalConnect har tagit fram i samarbete med cybersäkerhetsföretaget Truesec.

Den grundläggande idén med ransomware är att lägga beslag på kritiska data för att kunna kräva betalt av den som utsatts för att återställa eller lämna tillbaka uppgifterna. När intrånget är ett faktum kan den drabbade organisationens nätverk behöva ligga nere i flera veckor. Att återställa it-miljön helt och hållet för att komma tillbaka till en normal verksamhet tar många månader. Men med god grundläggande it-hygien, liksom bra verktyg och rutiner, kan du inte bara förebygga många incidenter. Du lindrar också de skadliga effekterna när något väl händer, och kan snabbare komma tillbaka till en fungerande verksamhet.

Tre vanliga vägar in vid en ransomwareattack

1 Kända sårbarheter

Att utnyttja en befintlig sårbarhet som har läckt ut gick nyligen om phishing som det vanligaste sättet att ta sig in i plattformar och nätverk. Exempel på sårbarheter kan vara säkerhetsbrister som uppstått i samband med en bristfällig integration, eller helt enkelt inloggningsuppgifter som kommit på villovägar. Idag finns system som automatiskt söker efter sårbarheter att utnyttja, och när en ny säkerhetslucka uppstår finns den i regel på hackarnas radar inom 72 timmar. När intrånget kommer går det snabbt: från initialt fotfäste till full kryptering på under två timmar. Väl på insidan kan angriparen lära känna nätverket och gradvis eskalera sina privilegier med målet att få globala adminrättigheter. Lyckas man med det kan man stjäla all data man vill och även slå ut eventuella backuper.

2 Phishing

Även den som säger att den aldrig skulle klicka på en länk i ett phishing-mejl kommer förmodligen att göra det förr eller senare. Aktörerna har blivit otroligt skickliga på att skapa meddelanden som ser ut att komma från en trovärdig källa. Visst är det bra att informera medarbetarna om hur de känner igen phishing-försök, men betydligt viktigare är att ha en plan för när någon har klickat.

3 Insiders

Den mänskliga faktorn är alltid en risk. Det förekommer till exempel att cyberbrottslingar mejlar medarbetare för att hitta någon som, i utbyte mot en stor summa i kryptovaluta, kan tänka sig att lägga en fil på ett usb-minne och lämna den i en dator någonstans på kontoret. Eftersom allt sker digitalt behöver medarbetaren inte ha någon direktkontakt med angriparna, utan kan få sin belöning genom att uppge rätt kod på en länk.

[1] https://www.svt.se/nyheter/inrikes/it-sakerhetsexpert-cyberbrottslighet-blir-storre-an-droghandeln

Nio sätt att motverka intrång

För att skydda din organisation mot ransomwareattackernas skadliga effekter behöver du jobba med förebyggande åtgärder. Det långsiktiga målet är att bygga upp en säker och stabil it-miljö. Du behöver också ha verktyg och rutiner på plats för att kunna upptäcka och respondera på angreppsförsök. Och om du råkar ut för ett fullbordat intrång där angriparna begär lösensumma: betala inte. Det leder ytterst sällan till att du får datan tillbaka.

1 Minimering av attackytan

En grundläggande säkerhetsåtgärd är att begränsa organisationens attackyta så mycket som möjligt. Attackytan är alla platser där en angripare skulle kunna ta sig in – från fysiska enheter som datorer och skrivare till molnlagrade filer. Även medarbetare är möjliga attackytor. De kan möjliggöra intrång genom till exempel bristande lösenordshantering och genom olika former av social manipulering, där de förmås att lämna ifrån sig uppgifter eller klicka på skadliga länkar.

Att minska attackytorna handlar bland annat om att begränsa åtkomster till olika system, liksom att löpande analysera och övervaka potentiella sårbarheter för att kunna upptäcka avvikelser i tid.

"Härda allt som går mot internet" är också en bra tumregel här. Du bör alltså säkerställa att alla operativsystem, programvara, nätverkskomponenter, databaser och andra applikationer konfigureras på ett säkert sätt.

2 Lifecycle management

Att jobba aktivt med lifecycle management, eller livscykelhantering, kan låta lite tråkigt men är absolut nödvändigt. När du systematiskt håller koll på status, användare, behörigheter med mera för både hårdvara och mjukvara minskar du risken för potentiella intrång. Se det som ett proaktivt underhållsarbete som lönar sig i längden. Här ingår också att hålla alla system uppdaterade så att eventuella sårbarheter som leverantören har upptäckt kan täppas till.

3 Multi-factor Authentication

MFA (Multi-factor Authentication), eller flerfaktorsautentisering på svenska, är ett effektivt sätt att se till att rätt person kommer åt rätt miljöer. Extra säkert blir det om användaren behöver knappa in en sifferkod från ett verktyg i sin mobiltelefon för att kunna logga in.

4 Lösenordsfri inloggning

Människor är notoriskt dåliga på att komma ihåg lösenord, särskilt om de är starka. Många använder dessutom samma lösenord på olika ställen. Jobba därför passwordless i så stor utsträckning som möjligt med hjälp av verktyg som möjliggör säker lösenordsfri autentisering.

5 Segregerade identiteter

Den som har global adminbehörighet ska bara använda dessa inloggningsuppgifter när det verkligen behövs, och gärna så sällan som möjligt. I mer vardagliga sammanhang ska ett separat användarkonto med lägre behörighet användas. Detta minskar risken för att kritiska adminrättigheter hamnar i fel händer.

6 Segregerade nätverk

Genom nätverkssegmentering, alltså att segregera de olika nätverk som organisationen använder,

> **"Om du råkar ut för ett fullbordat intrång: betala inte lösensumman!"**

bidrar du till att minska den potentiella räckvidden av en ransomwareattack. Det kan låta krångligt, men behöver inte vara det med rätt hjälp. Dessutom är den trista sanningen att det som är enkelt att administrera också är enkelt att ta över.

7 Skyddade backuper

Det kan låta självklart men tål att understrykas: ha inte backuper av alla kritiska tillgångar på ett enda ställe, och särskilt inte oskyddade.

8 EDR-system – och kompetent personal

Det räcker inte att hålla koll under kontorstider; övervakningen behöver ske i realtid dygnet runt. EDR (Endpoint Detection and Response) är en typ av mjukvara som kontinuerligt övervakar och analyserar filer och program. Med hjälp av AI kan potentiella hot upptäckas och rapporteras – och i vissa fall även åtgärdas. Men förlita dig inte helt på automatiken. Låt duktiga analytiker gå igenom alla larm för att avgöra hur allvarliga de är och vilka åtgärder som bäst kan desarmera dem.

9 Patchning

Sist men inte minst: patcha direkt. När du upptäcker en sårbarhet är det viktigt att patcha inom 24 timmar för att täppa till säkerhetsluckan. Annars kommer den garanterat att hittas och exploateras av angripare.

För att summera:

1. Minimera attackytan
2. Jobba med lifecycle management
3. Använd MFA (Multi-factor Authentication)
4. Kör lösenordsfri inloggning när det går
5. Sätt upp segregerade identiteter
6. Använd segregerade nätverk (nätverkssegmentering)
7. Skydda dina backuper
8. Använd EDR (Endpoint Detection and Response)
9. Patcha direkt om en sårbarhet upptäcks

Om GlobalConnect

GlobalConnect är den ledande leverantören av fiberbaserad datakommunikation och datacenter i norra Europa. Vi jobbar även med säkra nätverk, brandväggar och en stabil it-infrastruktur för våra 30 000 företagskunder. Kort sagt så gör vi det mesta inom uppkoppling. Men vad som är ännu viktigare är vårt starka engagemang, enorma kundfokus och mål att förenkla för er verksamhet. Läs mer på globalconnect.se.