

Innehållsförteckning

Hotbedömning och analys med Kill Chain -----	2
Reconnaissance -----	2
Weaponization-----	3
Delivery-----	4
Exploitation-----	5
Installation -----	7
Command & Control (C2) -----	7
Action on Objectives -----	8
CIA-triaden och påverkan på systemets säkerhet -----	9
Confidentiality -----	9
Integrity-----	10
Availability -----	10
Åtgärdsplan baserad på de fem principerna -----	11
Defense In-Depth -----	11
Least Privilege -----	11
Separation of Duties-----	11
Security by Design -----	12
KISS -----	12
Juridiska och etiska överväganden-----	12
Reflektion och långsiktig förbättringsplan-----	14
Diskussion-----	16
Källor -----	17

Teodor Fredriksson

Inlämningsuppgift 2: Cybersäkerhetsrisker, incidenthantering och strategier

Hotbedömning och analys med Kill Chain

Reconnaissance

Rekognoseringsfasen är kort sagt den inledande fasen i en cyberattack där angriparen försöker samla in så mycket information om måltavlan som möjligt. Oftast sker detta inledningsvis genom s.k passiv rekognosering för att sedan gå över till aktiv rekognosering. Den passiva fasen kan innebära att man söker efter information om måltavlan som finns offentligt tillgänglig. Det kan vara personuppgifter som finns på LinkedIn, en emailaddress kopplad till ett öppet konto på Instagram eller kända leverantörer som samarbetar med företaget.

När det går över till den aktiva fasen kan det betyda att man initierar någon form av kommunikation där tidigare erhållen information om måltavlan används för att iscensätta en situation där känsliga uppgifter kan byta ägare utan att måltavlan ifrågasätter angriparens motiv. Den erhållna informationen skulle också kunna användas för att på längre sikt bygga en relation och på det sättet utöva social engineering.

I fallet med ransomware-angreppet mot företaget SecureCom där det skett en riktad phishing-attack mot en anställd på företaget, också kallat för spear phishing, för att i slutändan få tillgång till den anställdes emailkonto, kan vi ponera att den inledande fasen har sett ut på följande vis:

- Angriparen skannar efter personliga uppgifter kopplade till företaget genom att läsa igenom tidigare publicerade pressmeddelanden, anställdas sociala medier och företagets webbsida.
- Angriparen hittar en anställd med öppen emailaddress på LinkedIn, och genom företagets webbsida väljs en av deras största leverantörer som bete.
- Angriparen skapar ett phishing-mail, som ex liknar ett standardutskick från leverantören som sker 1 gång i veckan. Genom att den anställda interagerar med emaillet laddas ex ett keylogger-virus ner alternativt att knappen leder vidare till en sajt som liknar leverantörens där den anställda skriver in sina användaruppgifter som sedermera skickas till angriparen.

Koppling till CIA-triaden

I detta fall har 'Confidentiality' inte följts. Man hade kunnat önska att det vore svårare i detta scenario för angriparen att få tag i den anställdes emailadress. Men, det skulle även kunna vara så att företagets leverantör i fråga inte heller har följt rekommendationerna för 'Confidentiality', vilket gjort att man kunnat replikera ett veckomail och potentiellt även imitera en anställd hos leverantören för att vagga in den anställda hos SecureCom i en falsk trygghet. Denne hade kanske reagerat om ett "ovanligt" namn i mailtråden dök upp med en anvisning att "logga in här på portalen".

Koppling till de fem säkerhetsprinciperna

- **Security By Design** – I och med att man inte har följt CIA-triaden har man inte lyckats få in säkerhet i grunden

Åtgärder

- Implementera policies för hur personlig och företagsrelaterad information får visas upp digitalt och analogt (ex visitkort)
- Implementera rutiner för att säkerställa att policies efterlevs

Weaponization

Weaponization syftar till den skadliga payloaden som levereras till målet. Payloaden består typiskt sett av en exploit och en malware, enligt Lockheed Martin.

- **Exploit** - Program som utnyttjar en säkerhetsbrist i systemet
- **Malware** - Program eller kod designad att ta över, förstöra eller förhindra system och datorer
- **Payload** – Skadlig kod som körs på målets system

I detta scenario skulle man kunna säga att exploiten är den anställda som har fallit för ett phishing-mail. Alltså, den mänskliga faktorn är i detta fall säkerhetsbristen i systemet. Den fejkade leverantörswebbsidan skulle kunna klassas som malwaren, designad att ta över kontrollen från användaren. Det kan dock även syfta till framtida utnyttjanden i attacken, som ännu inte ägt rum. I fallet med payload så skulle ex skadlig kod i form av en keylogger kunna laddas ned i samma veva som den anställda klickar på knappen i emaillet för att gå till webbsidan. Det kan även vara så att payloaden i form av skadliga kod som krypterar innehåll i en databas levereras vid ett senare tillfälle - eller, lagras latent på den anställdes enhet för att

sedan spridas vidare till andra enheter efter att angriparen har rört sig lateralt genom systemet och tillskansat sig ytterligare systemrättigheter.

Koppling till CIA-triaden

- **Confidentiality & Availability** – I detta fall är det inte företaget i sig som brustit mot något, men både 'Confidentiality' och 'Availability' hotas indirekt genom att angriparen förbereder en attack vars syfte är att kryptera information i utbyte mot lösensumma, med löfte att sprida och förstöra information om inte kravet uppfylls.

Koppling till de fem säkerhetsprinciperna

- **Defense In-Depth (härefter förkortat DID)** – Ett av de flertal lager som ingår i DID är utbildning för att motverka ex (spear)phishing.

Åtgärder

- Utbildningar för personal inom social engineering och phishing

Delivery

Delivery innebär analysen angriparen gör för att hitta mest lämpliga sätt för att leverera payloaden. Det kan ske genom att sprida USB-stickor infekterade med virus. Ironiskt nog verkar det vara relativt vanligt inom pentesting att man som ett första test bara kastar ut massa USB-stickor runt omkring på parkeringsplatsen vid företaget i fråga, för att se ifall någon anställd av ren nyfikenhet (och idioti) pluggar in USB:et i sin företagsdator. Man kan även använda sig av en s.k watering hole attack som går ut på att utnyttja en brist hos ex en webbplats som en specifik grupp ofta besöker, för att sedan omdirigera trafiken till en skadlig version av webbsidan. I detta fall verkar dock ett phishing-email vara valet av kontakt för angriparen.

Koppling till CIA-triaden

- **Confidentiality** – Hotas när användaren indirekt ger ut känslig information genom en spear phishing-kampanj

Koppling till de fem säkerhetsprinciperna

- **DID**– I och med att det enbart krävs ett användarnamn och ett lösenord så saknas här många lager av säkerhet, ex MFA.

Åtgärder

- **Utbildning** - Än så länge är vi fortfarande på angriparens planhalva, där SecureCom är omedvetna om att angreppet håller på att genomföras. Men bara för att man är omedveten behöver det inte betyda att man är blind inför risken att det sker. Därför återkommer vi till behovet av just utbildningar för att förebygga den mänskliga faktorn.

Exploitation

Vid det här laget kan vi anta att den anställda har klickat på mailet och skrivit in sina uppgifter, som har skickats tillbaka till angriparen. Nu kan angriparen utnyttja det faktum att systemet inte har någon MFA. Baserat på användaruppgifterna kan angriparen även analysera två saker: om det finns policies för starka lösenord, och policies för användarnamn.

Låt oss leka med tanken att det inte finns policies för starka lösenord, men det **finns** policies för uppdatering av lösenord med 1 månads mellanrum. Det finns även policies för användarnamn. I fallet med denna anställda låtsas vi att uppgifterna ser ut som följande:

Användarnamn: Erik.haaf@foretag.support.se

Lösenord: April2025

Angriparen vet nu två saker, och kan anta en tredje – det krävs inga starka lösenord med tanke på längden och bristen på specialtecken. Och mailen består av förnamn, efternamn, företagets namn och den anställdes roll inom företaget, separerade med punkter. Lösenorden verkar dessutom bytas så pass ofta att anställda har tappat sin kreativitet - därav att lösenordet består av den faktiska månaden och året som attacken sker.

Utöver att angriparen nu har tillgång systemet och kan börja kryptera innehåll, kan denne nu även sätta igång en Brute Force-attack för att knäcka andra konton med högre behörigheter.

Användaruppgifterna **Kilona.Stromstedt@foretag.admin.se / April2025** ger angriparen en träff! Och det med adminrättigheter till systemet. Angriparen lyfter upp det ursprungliga kontot som dessutom innehåller den skadliga payloaden, och ger kontot adminrättigheter. Nu kan angriparen börja förbereda sig för att kryptera större delar av systemet.

Koppling till CIA-triaden

- **Confidentiality** – Bryts allt mer ju mer uppenbart det blir att DID inte har följts nämnvärt. Nu riskerar flera konton att komprometteras.
- **Integrity** – Med adminrättigheter kan nu angriparen manipulera hela systemets data, inklusive andra användares.
- **Availability** - Löper nu en hög hotrisk med tanke på adminrättigheterna och den latent a ransomwaren.

Koppling till de fem säkerhetsprinciperna

- **DID**
 - Det fattas MFA, vilket har möjliggjort för angriparen att inte bara ta över ett konto, utan även ett adminkonto, vilket har gjort att angriparen kan börja röra sig lateralt inom systemet.
 - Företaget har grundläggande antiviruskydd, men eftersom ransomwaren i detta fall verkar ha gått obemärkt förbi kan det mycket väl vara så att det saknas rutiner för systemuppdateringar vilket har möjliggjort för payloaden att utnyttja en säkerhetsbrist i en gammal version.
- **Least Privilege**
 - Det faktum att angriparen har kunnat röra sig lateralt kan vi se som resultatet av en kombination med otillräckligt åtkomstbegränsning, utbildning och säkerhetspolicies.
- **Separation of Duties**
 - I detta fall räckte det med ett adminkonto för att ge rättigheter till hela systemet. Lite utav ett "One Access Right To Rule Them All"-scenario.
- **KISS**
 - Användarnas svaga lösenord är en indikation på ett alltför monotont schema för lösenordsändring, utan stöttande policies som stärker användandet av starka lösenord.
- **Security By Design**
 - Kombinationen av ovan brister tyder på att säkerhet inte har legat i fokus vid byggandet av systemet.

Åtgärder

- Implementera MFA(2FA)
- Uppdatera policies för lösenord för att säkerställa att starka lösenord används
- Tydligare rollfördelning. En admin kanske bara ska vara admin för en viss grupp av anställda
- Implementera rutiner för systemuppdateringar, inte minst av antivirusprogram

- Om företaget har någon form av notissystem vid uppdatering av användares systemrättigheter hade man här kunnat gå in och stänga av komprometterade användare för att begränsa spridningen av viruset.

Installation

I detta steg har angriparen som mål att säkerställa att det finns en s.k backdoor in till systemet ifall angriparen skulle bli utlåst, eller om enheten startas om. Med tanke på att detta är en ransomware-attack och angriparen förmodligen vill kryptera så mycket data som möjligt på en och samma gång, för att på så vis förbli oupptäckt under så lång tid som möjligt, kan vi anta att angriparen tänker använda sig av en [Meterpreter](#). Det ger angriparen möjlighet att utföra kommandon på den anställdes infekterade enhet på avstånd, och på så sätt köra den skadliga koden vid bästa(värsta) möjliga tillfälle.

Koppling till CIA-triaden

- **Integrity** – Med kontinuerlig tillgång till känslig information löper företaget stor risk för att dess integritet förgörs genom spridning, manipulering eller förstörelse.
- **Availability** - Här löper företaget stor risk för en total kollaps om tillräckligt mycket data krypteras samtidigt.

Åtgärder

- Här hade NDR varit mycket användbart för att upptäcka misstänksamma mönster i nätverkstraffiken och på så sätt få nys om ett angrepp.

Command & Control (C2)

C2 är upprättande av kommunikation mellan enheten och angriparens server, genom ex Meterpreter som jag nämnde tidigare. Om denna koppling upprättas innebär det att angriparen har full kontroll över den infekterade enheten och kan bland annat göra följande:

- Uppdatera den skadliga koden
- Hämta ny kod
- Exfiltrera filer, som ex databaser
- Initiera kryptering av filer

Koppling till CIA-triaden

- **Confidentiality** – Med en direkt koppling mellan den infekterade enheten, systemet och C2-servern kan känslig information forslas ut till förmån för angriparen.
- **Integrity** – Med tillgång till systemet genom C2-kanalen kan angriparen manipulera databasen, ändra användares rättigheter samt skapa nya användare.
- **Availability** – Om krypteringen av systemets känsliga information inte redan är initierad så löper företag en överhängande risk för att det kan ske när som helst i detta stadie.

Koppling till de fem säkerhetsprinciperna

- **DID** - Företaget saknar NDR. Med NDR hade man kunnat oregelbunden nätverkstraffik och flagga för en pågående säkerhetsrisk.
- **Separation of Duties** – Pga adminanvändarens överdrivna rättigheter har lateral rörelse kunnat ske och lagt grunden för en perfekt enhet med lika stor systemrättigheter att upprätta en C2-kanal ifrån.

Åtgärder

- Implementera NDR för att analysera misstänksam nätverkstraffik
- Implementera EDR för att analysera misstänksamt beteende från de infekterade enheterna
- DNS-filtrering. De vanligaste C2-kanalerna som används vid cyberattacker är idag kända, och hade kunnat blockeras genom brandväggen

Action on Objectives

Det är här som effekten av angreppet blir otvetydigt för företaget. Efter att angriparen har klättrat lateralt inom systemet och satt upp en C2-server kan stora delar av databasen krypteras i en och samma smäll.

Koppling till CIA-triaden

- **Confidentiality** – De känsliga uppgifterna företaget besitter är i denna stund de facto inte längre konfidentiella – de tillhör nu även angriparen.
- **Integrity** – Alla nödvändiga kanaler för att förstöra, modifiera och exponera uppgifterna är angriparen till hands.

- **Availability** – Med den skadliga koden redo att köras på stora delar av systemet är en systemkollaps bara en tidsfråga.

Koppling till de fem säkerhetsprinciperna

- **Security By Design** - Företaget har brustit på ett antal olika fronter:
 - Lösenordshantering
 - MFA
 - Åtkomstloggning
 - Segmentering
 - EDR/NDR
 - Utbildning
 - Systemuppdateringar
 - Externa/Interna Backups (Vad jag har kunnat läsa i alla fall)
 - Användarrättigheter
 - Policies för offentligt delad information

Åtgärder

Nu antar vi att företaget har upptäckt skadan, och detta är vad de bör göra:

- Isolera infekterade enheter
 - Stäng av enheterna
 - Ta bort alla befogenheter från de infekterade/nyskapade kontona
- Informera och anmäla attacken enligt GDPR
- Man måste väl anta att ett företag som jobbar med molnbaserade lösningar faktiskt **har** backups, åtminstone delvis via sin externa leverantör? I så fall bör man stegvis återställa systemet via dessa **efter** att det bekräftats att skadliga aktörer är tillräckligt isolerade.
- Analysera och dokumentera händelseförloppet

CIA-triaden och påverkan på systemets säkerhet

Confidentiality

Angreppet har på flera sätt brutit mot principerna som definierar Confidentiality. Genom phishing har angriparen fått åtkomst till inloggningsuppgifter och därmed känslig kundinformation, kontrakt och interna dokument. I och med att angriparen hotar att publicera den känsliga datan innebär det att datan har förlorat sin konfidentialitet.

Åtgärder

- Begränsa anställdas åtkomst till det mest nödvändiga och inget mer (Least Privilege, Separation of Duties)
- Implementera MFA för att skydda autentisering (Least Privilege, DID)
- Införa säkerhetsträning för att minska phishingrisk (DID)
- Uppdatera anti-virusprogram (DID)

Integrity

Med adminbehörighet kan angriparen manipulera användarkonton, systeminställningar och innehåll i databaser. Företaget kan därför inte längre garantera att informationen är korrekt eller oförändrad. Även efter återställning är det svårt att veta exakt vad som har modifierats.

Åtgärder:

- Införa digitala signaturer/loggning för att upptäcka ändringar (Security by Design, DID)
- Begränsa adminåtkomst (Least Privilege, Separation of Duties)
- Regelbunden integritetsvalidering av databasinnehåll (DID)
- EDR för att upptäcka ovanlig aktivitet på endpoints (Security by Design)
- Policies och regelbundna rutiner för ändring av starka lösenord (DID, KISS)

Availability

Ransomware har gjort en stor del av företagets system och data otillgänglig. Angriparen har även lyckats kryptera säkerhetskopior, vilket förvärrar situationen. Affärsprocesser har stannat och kunder har börjat klaga.

Åtgärder:

- Ha air-gapped backups för att förhindra vidare kryptering genom nätverk
- Segmentera nätverk så att ett angrepp inte sprider sig till hela IT-miljön
- Rutiner för isolering av infekterade enheter
- Öva återställning så att system snabbt kan komma tillbaka online

Källor: [Fortinet](#)

Åtgärdsplan baserad på de fem principerna

Defense In-Depth

Flera lager av säkerhet hade kunnat stoppa angreppet redan i ett tidigt skede. Bristen på övervakning (NDR/EDR), saknaden av e-postfilter, anti-spoofing och frånvaron av MFA skapade en sårbar säkerhetskedja

Åtgärder:

- EDR och NDR för beteendeanalys
- MFA på alla externa och interna inloggningar
- Utbildningar för personal om phishing och social engineering
- Regelbundna penetrationstester och sårbarhetsskanningar

Least Privilege

Flera användare hade för breda rättigheter. Angriparen kunde därför röra sig lateralt och uppgradera den ursprungliga användaren till administratörsbehörighet.

Åtgärder:

- Införa rollbaserad åtkomst (RBAC)
- Säkerställa att endast de som behöver adminrättigheter har det
- Regelbunden granskning av behörigheter
- Automatisk notifikation vid behörighetsändringar

Separation of Duties

Ett enskilt adminkonto kunde påverka hela miljön. Det finns inget system där flera personer måste godkänna känsliga ändringar eller där ansvar är uppdelat.

Åtgärder:

- Implementera principen om delat ansvar vid kritiska systemändringar
- Skapa roller för revision, godkännande, och genomförande
- Införa granskningsloggar där ingen kan redigera sina egna spår

Security by Design

Systemen verkar ha byggts utan tanke på att skydda mot moderna hot. Avsaknaden av segmentering, säker autentisering och dataskydd visar att säkerhet inte varit en prioritet vid utformning av den digitala infrastrukturen.

Åtgärder:

- Kartlägga hela systemmiljön och identifiera risker
- Omstrukturera IT-arkitekturen med säkerhet som grundpelare
- Säkerställa att externa molntjänster uppfyller branschstandarder
- Sätta upp handlingsplan för att jobba mot ISO 27001

KISS

Uttjatade lösenordsrutiner och med otillräckliga policies som stöttning har lett till att enkla mönster har följts vid nyskapande av lösenord.

Åtgärder:

- Införa lösenordshanterare för att minska bördan på användarna
- Implementera MFA
- Ha tydliga och stöttande säkerhetspolicies som minskar risken för fel genom den mänskliga faktorn

Källor: [Abnormal](#), [IT Governance](#)

Juridiska och etiska överväganden

I och med att SecureCom har utsatts för ett dataintrång där personuppgifter har läckt ut ställs per automatik ett flertal krav på företaget enligt GDPR. Dessa krav gäller alla företag, oavsett

storlek, om de behandlar personuppgifter inom EU. Det innebär alltså att även företag utanför EU som hanterar personuppgifter med koppling till innanför EU måste rätta sig efter detta. Misslyckas man med att följa GDPRs direktiv riskerar man höga böter på upp till 2% eller 4% av företagets årsomsättning, eller 10 eller 20 miljoner euro ([IT Governance](#)). Enligt artikel 33 och lagkrav i Sverige ska incidenter som rör personuppgifter och som kan anses skadliga för användarna anmälas inom 72 timmar till insynsmyndigheten IMY ([artikel 33](#)).

SecureCom har även ett ansvar och ett krav på sig enligt artikel 34 ([artikel 34](#)) att kontakta användare vars uppgifter har läckt om dessa läckor anses löpa hög risk för att påverka personernas friheter och rättigheter.

Om vi ska tackla det analytiska, kanske mer subtila, utifrån attacken så är det mer än höga böter som står på spel för företaget. Till att börja med så har vi själva lösensummakravet på 200 000 euro som ställts från attackgruppen. Även om det kan kännas lockande och tryggt att bara få tillbaka all sin information så är det som med vilken utpressningssituation som helst – vad är det som hindrar de från att göra om det igen, och denna gång med ett ännu högre lösenkrav? De vet ju att du kunde betala förra gången, och snabbt gick det. Så då kan du säkert göra det igen. Utöver det måste man fråga sig följande:

- Vad har du för garantier att du faktiskt får tillbaka all din data?
- Kan du vara säker på att datan inte redan har spridits? I så fall, känner betalningen av lösensumman fortfarande samma ursprungliga syfte?
- Pengarna går troligtvis till att fortsätta stötta kriminella organisationer. Är du villig att stötta det ur egen ficka?
- Blir du verkligen fri från dina förpliktelser gentemot GDPR om du betalar för att få tillbaka din datan “oskadd”? Enligt GDPR måste du fortfarande anmäla händelsen och riskerar fortfarande böter.

Det kan kännas som det “billigare” alternativet att bara betala och tänka “skönt, nu är det över”. Men även om vi åsidosätter GDPRs krav på anmälan av incident så bör man ta i beaktning vad som kan hända med ens rykte om det skulle komma fram, vilket det sannolikt gör förr eller senare, till dina kontraktskunder, eller myndigheter för den delen.

Personligen hade jag inte velat betala en leverantör som undanhållit för mig att mina kunduppgifter hos de hade blivit stulna utan att jag som målsägare fått veta det. Det öppnar även upp för en ny hävstång i en ny utpressningshärva - och denna gång krävs inte ens en Cyber Kill Chain för att genomföra attacken. Det räcker med några bilder från företaget och attackgruppens förhandling om överföringen av det krypterade innehållet.

Som potentiellt blivande kund hade jag lagt alla planer på en upphandling hos leverantören på is om jag fick reda på att de försökt dölja en cyberattack för sina befintliga kunder. Ett ödesdigert beslut, kan tyckas.

Vidare verkar Cybersec-världen överens om att **aldrig** betala lösensumma till ransomware-attacker. Att agera i enlighet med detta stärker kollektivets passiva försvar gentemot den här typen av cyberattacker. Men om enskilda aktörer fortfarande väljer att betala så visar man indirekt att det fortfarande är lönt för hackergrupper att syssla med den här typen av utpressning.

Källor: [IT Governance](#), [Privacy Regulation](#), [GDPR-Text](#), [Hycu](#), [Legal](#)

Reflektion och långsiktig förbättringsplan

Attacken möjliggjordes till synes pga en anställds oförmåga att identifiera en s.k threat actor. Det är inte otänkbart att man från ett företagsperspektiv avfärdar eller till och med lägger skulden för händelsen på den enskilde anställda. Men ett gediget säkerhetstänk med rutiner, rollfördelningar och kunskap börjar med ledningen. Det verkar även otydligt vem som ansvarar över vad under detta angrepp. Förutsatt att det är så i praktiken så förlorar man väldigt dyrbar tid om resurser måste läggas på att reda ut "vem som gör vad" under en pågående attack.

Det finns förbättringspotential inom varje säkerhetsprincip och bristerna påverkar tillsammans helheten av CIA-triaden. Även om det krävs åtgärder inom såväl rutiner som systemimplementeringar så känns det som att det framförallt krävs en förändrad inställning anpassad efter moderna säkerhetsrisker.

Åtgärder

1. Teoretisk kompetens & utbildningar

- Genomför rutinemässiga utbildningar inom:
 - Phishing
 - Brute-Force
 - Social Engineering
 - Implementera som en del av onboarding. **OBS! Viktigt att repetera utbildningen med regelbundna intervaller**
- Skapa ett schema med tydlig rollfördelning. I händelse av X bör alla veta att person Y är ansvarig för uppföljning. Om person Y saknas bör en efterträdare redan finnas utnämnd så att processer kan fortgå utan avbrott.

2. System & teknik

- En sårbarhetsskanning bör köras omgående för att identifiera "långt hängande frukt" såsom oanvända öppna portar i nätverket, utdaterade versioner av operativsystem, tjänster utan MFA, konton med defaultlösenord som ex "admin/admin"
- Implementera MFA på alla tjänster kopplade till företaget
- Implementera EDR
 - Välj leverantör - förslagsvis CrowdStrike
 - Installera agenten på företagsenheter
 - Konfigurera vad som ska flaggas som "onormalt beteende", som exempelvis:
 - Osignerade program
 - Processer som försöker kryptera stora mängder data
 - Låt EDR använda sig av maskininlärning för att lära sig de anställdas digitala beteendemönster (begränsa självklart till företagsenheter)
 - Koppla informationsflöde från EDR till SOC-teamets SIEM-program (ex, Microsoft Sentinel)
- Sätt upp accessloggning
- Säkerställ att loggar inte kan redigeras av den som orsakat loggen
- Sätt upp årlig rutin för pentesting

3. Kommunikation

- Etablera mall för kommunikation med myndigheter, personal och kunder vid säkerhetsincident.

4. Kvalitetssäkring

- Jobba utifrån ramverket ISO 2007

Riskmatris

Risk	Sannolikhet	Konsekvens	Prioritet	Åtgärd
------	-------------	------------	-----------	--------

Phishing	5	5	25	Inför regelbundna säkerhetsutbildningar // Inför email-filter
Obehörig åtkomst i system	5	5	25	Inför MFA på alla system
Eskalerad behörighet genom lateral rörelse	5	5	25	Upprätta tydlig rollfördelning och separera behörighet i system i enlighet med 'Least Privilege'
Kryptering och förstörelse av känslig information	5	5	25	Inför EDR/NDR // Segmentera nätverk // Inför rutin för backup
Dålig översikt av IT-säkerheten	5	3	15	Inför regelbunden sårbarhetsskanning
Otydlig incidentplan	5	3	15	Konkretisera mallar och scheman för agerande vid varje fas enligt IRP

Diskussion

Tanken bakom de risker jag bedömt som kritiska har till stor del med dess tekniska symbios att göra, och konsekvensen av otillräckliga lager av säkerhet. Om MFAs, EDR och tydligare rollfördelning hade funnits på alla system så hade risken varit fortsatt hög pga låg utbildningsnivå inom ämnet hos personalen, men konsekvensen av ett komprometterat användarkonto hade inte blivit densamma. MFA hade kunnat hindra en inloggning från att ske

över huvud taget. EDR hade kunnat blocka användaren vid första tecken på avvikande beteende eller segmentera användaren från nätverket. Ett användarbehörighetssystem enligt RBAC hade fortfarande kunnat åsamka företaget och dess användare skada, men potentialen för skadan hade varit avsevärt mindre.

Man kan byta ut phishing i detta scenario mot vilken som helst av de kritiska riskerna, och effekten blir densamma – farlig i brist på avsaknaden av de andra kritiska resurserna, vars skadliga potential drastiskt minskas för varje implementering.

De riskerna med lägre prioritet är sådant som jag skulle säga är mer diffusa i sin förväntade effekt. En sårbarhetsskanning kan vara väldigt positivt för att identifiera säkerhetsbrister, men det faktum att man gör en säkerhetsskanning resulterar inte nödvändigtvis i att säkerheten förbättras. Implementering av ex MFA har en direkt korrelation mellan agerande och mätbart värde. En säkerhetsskanning är fortfarande något jag rekommenderar i detta scenario, men framförallt för att företaget ska skapa sig en tydligare uppfattning om vart de ligger med sin IT-säkerhet.

En otydlig IRP är inte heller nödvändigtvis kritiskt. SOC-teamet kan mycket väl fungera bra under press. Den känns som att den största risken med en obefintligt eller otydligt IRP är att resultatet från situation till situation blir osäkert. Frågan blir ifall rätt person är på rätt plats. En IRP hjälper till att konkretisera vad som gör vad, när och hur och kan i slutändan minimera förlust av data eller skada på system och i långa loppet - företags rykte, status och ekonomi.

Källor

- [Fortinet](#)
- [Abnormal](#)
- [IT Governance ISO](#)
- [IT Governance GDPR](#)
- [Privacy Regulation](#)
- [GDPR-Text](#)
- [GDPR Artikel 33](#)
- [DPR Artikel 34](#)
- [Hycu](#)
- [Legal](#)