Vägledning

# Ransomware

ES2024-16

November 2024

Innehållsförteckning

# 1. Sammanfattning

## 1.1 Inledning

Vägledningen är framtagen med anledning av den ökande mängden ransomware[1]-attacker mot eSams medlemmar och svensk offentlig förvaltning.

Ransomware-attacker kommer sannolikt att drabba alla myndigheter förr eller senare, varför det är viktigt att ha beredskap för det. Förebyggande arbete är viktigt och ännu viktigare är att ha en god förmåga att återgå till ett normalläge efter en störning. Skyddsnivån behöver utvärderas för varje myndighet enskilt, men alla behöver ha förmåga att kunna hantera en ransomware-attack.

## 1.2 Syfte

Vägledningen är en guide och rådgivning för medlemsmyndigheter i eSam med syfte att stärka den egna förmågan att motstå ransomware-attacker. Den omfattar både egen och anskaffad it. Vägledningen och rekommenderade arbetssätt kan även stärka förmågan att motstå andra typer av cybersäkerhetsattacker, men det är inte ett huvudsyfte.

### 1.2.1 Avgränsning

Informationsmängder som faller under säkerhetsskydd och hantering av sådan information, beskrivs inte i denna vägledning.

## 1.3 Målgrupp

Primär målgrupp är personer vid eSams medlemsmyndigheter som arbetar med incidenthantering och skydd mot skadlig kod. Det kan även vara av intresse för personer i anskaffningsprojekt, jurister, it-tekniker, säkerhetsexperter, verksamhetsplanerare eller intresserade offentliganställda.

## 1.4 Medverkande

Följande myndigheter har deltagit aktivt i framtagandet av vägledningen: Arbetsförmedlingen (färdledare), Centrala Studiestödsnämnden, Domstolsverket, E-hälsomyndigheten, Ekonomistyrningsverket, Folkhälsomyndigheten, Länsstyrelserna,

[1] Definition av ransomware; https://sv.wikipedia.org/wiki/Ransomware

Migrationsverket, Naturvårdsverket, Pensionsmyndigheten, Skolverket, Statistiska centralbyrån, Tullverket och Universitets- och högskolerådet.

## 1.5 Disposition

Vägledningens struktur återspeglar ett händelseförlopp och eget rekommenderat arbetssätt vid angrepp och hantering av ransomware-incidenter:

- Förebygga, omfattar förebyggande åtgärder
- Upptäcka, omfattar förmåga att tidigt upptäcka skadlig kod
- Åtgärda, omfattar både att hindra den skadliga koden och att identifiera hur angreppet började
- Återställa, omfattar att den initiala sårbarheten åtgärdas och att system återställs till det skick de var före angreppet
- Lärdomar, omfattar en ständig förbättring av alla delar

# 2. Problembild kring ransomware och skyddsåtgärder

Ransomware har blivit ett samhällsproblem som ökat kraftigt över tid. En internationell studie från 2024 visar att 59 %[2] av tillfrågade organisationer säger sig ha blivit drabbade av ransomware attack senaste året. En annnan mätning visar på ökning av ransomware på 58 % från år 2023 till år 2024[3]. Ransomware är ett samhällsproblem. Det finns två huvudsakliga drivkrafter bakom attackerna; att störa samhället[4] och ren ekonomisk brottslighet. Oavsett syfte sänker attackerna förtroendet för samhällsfunktioner i allmänhet och för den berörda myndigheten i synnerhet. Flera av eSam medlemsmyndigheter har drabbats av ransomware-attacker.

Det är viktigt att utgå från myndighetens bedömning om krav och behov runt ransomware (skydd mot verksamhetsavbrott och dataförlust) vid inrättandet av sin motståndsförmåga och vald nivå av motståndskraft. Statliga myndigheter ska följa MSBFS 2020:7[5] och punkterna i föreskriften ger ett relevant grundskydd mot skadlig kod. Myndigheten ska även planera för myndighetens ålagda krav på rapportering och förmåga att rapportera incidenter enligt MSBFS 2020:8[6] och framöver även enligt kraven

[2] En global mätning kring ransomware; https://www.sophos.com/en-us/content/state-of-ransomware
[3] Trendrapport kring ransomware; https://www.trmlabs.com/post/ransomware-in-2024-latest-trends-mounting-threats-and-the-government-response
[4] SÄPO:s årsbok; https://cve.se/publikationer/sakerhetspolisen20232024.5.2da6bed18d824c5c7232cae.html
[5] MSBFS 2020:7 föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter. Länk
[6] MSBFS 2020:8 föreskrifter om rapportering av it-incidenter för statliga myndigheter. Länk

från NIS2-direktivet[7]. Men dessa krav är också bara minimikrav, flera myndigheter har egna högre krav.

Varje myndighet behöver hitta sin nivå av krav och arbetsprocess kring förebyggande, upptäckt, åtgärd och återställande av it-system. Detta bör kompletteras med ett arbetssätt för ständiga förbättringar. Självklart ska myndigheter också nyttja de centrala stödfunktioner som erbjuds myndigheter tex via cert.se som från insamlade kända incidenter från andra organisationer och myndigheter, kan varna och förhindra i förväg.

Ransomware-attacker påverkar hela myndigheten. Därför behöver hela verksamheten vara involverad i det förberedande arbetet, med att planera och öva enligt rätt beslutad nivå. Anskaffning eller etablering av it-stöd behöver föregås av en hot- och riskanalys samt rätt ställda krav tex kring kontinuitet, informationshantering och it-säkerhet.

Här följer en kort beskrivning av attackvektorer[8] och övergripande åtgärder:

## 2.1 Användarbeteende

Historiskt har angripare ofta attackerat enskilda användare, eftersom användare varit enklare mål än it-system. Detta görs exempelvis med phishing-mail, eller USB-stickor, se *bilaga 1 Inkomna filer och USB-minnen*. Skyddsåtgärden är att arbeta med säkerhetskultur och riktad utbildnig till medarbetarna om dessa typer av risker.

## 2.2 Kända sårbarheter

Ett tillvägagångssätt som ständigt ökar är när angripare använder sig av kända säkerhetshål, där det visserligen finns en säkerhetspatch, men angriparna räknar med att alla kunder inte hunnit implementera den. Skyddsåtgärden är att ha goda rutiner för att installera säkerhetsuppdateringar.

## 2.3 Okända sårbarheter

Det mest intrikata angrepssättet är att utnyttja en tidigare okänd sårbarhet. Metoden är sällsynt och går egentligen inte att skydda sig mot varför det är bra att utgå ifrån att angrepp kommer att ske och att etablera rutiner och processer för att hantera angreppen och återställa utsatta system.

[7] Network and Information Security Directive (NIS2). Länk
[8] Förklaring attackvektorer; https://www.techopedia.com/se/ordlista/attack-vector

## 2.4 Läckta lösenord

Konsekvenser av läckta lösenord drabbar allt fler alternativt där lösenord är för enkla och vanliga (så att de går att gissa). Lösenorden kan ha stulits vid ett tidigare angrepp eller läckts av personer på insidan. Det mest effektiva skyddet mot detta är att inte enbart förlita sig till användarnamn och lösenord utan att använda fler-faktor-inloggning samt övervakning av avvikande användarbeteenden.

# 3. Förebygga

Våren 2024 var den vanligaste attackvektorn förekomsten av kända sårbarheter som inte åtgärdats på grund av eftersatta säkerhetsuppdateringar. Tidigare har e-post med länkar till skadlig kod eller externa USB-stickor pekats ut. Vilken attackvektor som används mest kan variera över tid. Förebyggande arbete är alltid billigare och effektivare än att åtgärda i efterhand. Följande områden beskriver viktiga delskydd som tillsammans ger ett relativt gott skydd om det är korrekt hanterat.

## 3.1 Behörigheter och autentisering

Ett bra grundläggande skydd är att använda fler-faktors-inloggning för samtliga externt exponerade system. Vid ransomware-angrepp kan det ofta vara det bästa skyddet mot läckta eller köpta lösenord. Genom att centralisera behörighetsstyrningen säkerställs även att andra, sämre behörighetslösningar hindras från att användas i myndighetens olika system. Centraliserad behörighetsstyrning underlättar etablering av gemensam policy och behörighetsuppföljning.

Myndigheter bör ha en policy att kontonamn och lösenord för jobbkonton aldrig får återanvändas privat, då kontonnamn och lösenord ofta återanvänds överallt för enkelhets skull. Något som användas av antagonister. Myndigheten behöver minimera antalet administratörsbehörigheter och säkerställa regelbunden uppföljning samt att behörigheterna endast används för adminstration.

## 3.2 Säkerhetskopior

Vid ett ransomware-angrepp försöker antagonisten kryptera filer. Säkerhetskopior brukar vara ett prioriterat mål för att försvåra för den som utsätts för attacken. En kritisk framgångsfaktor för att kunna återställa kopian efter ett angrepp eller incident, är att se

till att säkerhetskopior inte kan manipuleras. Många verktyg för säkerhetskopior erbjuder skydd mot manipulation, genom lösningar som är ”Immutable” eller ”Write Once”. Hårdvarubaserade lösningar är att föredra då en antagonist sannolikt skulle behöva fysisk access till datorhallen där säkerhetskopior finns. Lås med enbart mjukvara kan potentiellt hackas via fjärraccess.

Förutom skydd mot manipulation behöver även åtkomstskyddet säkerställas på annan ort sepparerad från produktionsmiljö men det kan vara svårt om myndigheten saknar egen datorhall och nätverksförmåga över flera geografiska platser. Det är heller inte säkert att en it-sourcingpartner kan erbjuda detta i sitt it-landskap. Sådan förmåga är alltid kostnadsdrivande och kan prioriteras bort om det saknas tydliga beslutade krav om detta.

I MSBFS 2020:7 4 kap 14-15 §§ föreskriver MSB att myndigheten ska kunna återställa backup från regelbundet tagen säkerhetskopia och att säkerhetskopiorna ska förvaras skilt från produktionsmiljö samt skyddas från skada, obehörig åtkomst och obehörig förändring.

Myndigheten ska även hantera Riksarkivets föreskrifter och allmänna råd om elektroniska handlingar (RA-FS 2009:1)[9] som bland annat beskriver hantering och förvaring av säkerhetskopior för offentlig verksamhet och handlingar som är allmänna samt hur dessa ska kunna återställas.

### 3.2.1 Planering för säkerhetskopiering

Som nämnts i 3.2 är fungerande rutiner för säkerhetskopiering kritiskt för en god återställningsförmåga. För myndigheten kan det tillsammans med en ransomware innebära stora störningar i sitt myndighetsuppdrag. En ransomware attack kan slå på flera olika sätt för varje berörd organisation, hur myndigheten kan stå emot kan därmed behöva se väldigt olika ut. Kritisk verksamhet måste återupptas i begränsad omfattning för att t.ex. klara de viktigaste delarna i sitt myndighetsuppdrag även om hela miljön inte går att återställa lika skyndsamt. Beroende på hur attacken fortgår kan processen för att återgå se väldigt olika ut.

Generellt gäller att genom forensisk analys och behörighetsstädning kan förövarens åtgärder systematiskt stängas ner samtidigt som den isolerade (ingen access mot internet) återställningen pågår. Detta är en praktisk metod för att kunna återställa senaste myndighetsinformationen från en (misstänkt-) smittad backup. Myndigheten kan med

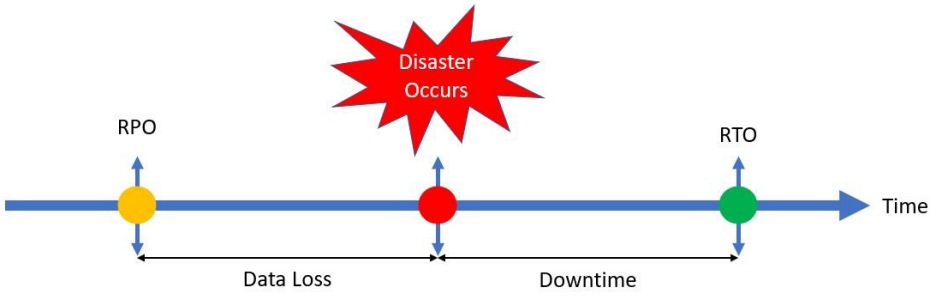
[9] https://riksarkivet.se/rafs?pdf=rafs%2fRA-FS+2009-01.pdf

fördel planera säkerhetskopiering kopplat till verksamhetsprioritering innan incidenten inträffar. Finns det topp prioriterade system och informationsmängder eller bara delar som bara måste fungera skyndsamt för myndigheten behöver denna säkerhetskopieringsplan känna till dessa. Framtagandet av denna plan behöver göras med god representation från påverkad verksamhet och verksamhetsförståelse.

Samtliga backup- och återställningsrutiner behöver både övas och verifieras så att organisationen bekräftat har förmåga att återställa en backup vid behov. I myndighetens planering behöver ingå hur länge backuper ska bevaras och hur frekvent de ska göras. Ju mindre säker förmågan att upptäcka angrepp bedöms vara, desto längre historik av backuper kan behövas för att minimera dataförlust vid en incident.

Om myndigheten helt skulle sakna fungerande backuper (att säkerhetskopior blivit korrupta) så måste it-förmågor och information återskapas från noll och utan historik. Det riskerar att bli väldigt resurskrävande och kostsamt och får stor inverkan på myndighetens förmåga att utföra sitt myndighetensuppdrag.

Myndigheten behöver beakta *Recovery Point Objective – RPO* och *Recovery Time Objective – RTO*[10] d.v.s. hur mycket information är myndigheten beredd att tappa och hur lång tid får gå för att komma igång igen tex vid en ransomware attack.




*Figur 1: Hur mycket data kan återskapas eller förloras och hur länge kan myndigheten klara sig utan olika informationsmängder samt It system. Källa manishsharma blogg.*

Tätare återställningspunkter kan innebära minskad dataförlust men kan ställa större krav på lagring och kan snabbt bli kostnadsdrivande. Myndigheten behöver överväga hur lång tid verksamheten kan acceptera för att återställa ett system vid en händelse. Exempelvis en dedikerad backuplösning för ett verksamhetssystem eller viss upphandlad tjänst istället för delad, men det ger också högre kostnad. Kärnfrågan som myndigheten

[10] https://en.wikipedia.org/wiki/IT_disaster_recovery

behöver ta ställning till, är kostnad mot eventuell dataförlust kontra den tid som systemet ligger nere.

### 3.2.2 Förvaring av säkerhetskopior

Förr togs säkerhetskopior på fysiska band som förvarades på annan plats än servrar och nätverk. Den gamla teknikens fysiska separation är något som fortfarande är önskvärt, samtidigt som nyare teknik är mindre arbetsintensiv och kräver en lägre grad av fysisk närvaro i en datorhall. När myndigheterna gick från magnetband som lagringsmedium för säkerhetskopior, till hårddisk-lösningar, separerades ofta produktionsnätet från underhållsnätet för att inte belasta produktionsnätet med säkerhetskopior. Idag är både servrar och nät ofta virtuella.

Det finns en mängd krav som är lämpliga att ställa på en lösning för säkerhetskopiering:

- Kopior ska inte förvaras i datorhallen för att undvika att de utsätts för samma fysiska risker som datorhallen, t.ex. brand eller översvämning.
- Säkerhetskopian ska ha åtkomstskydd och kryptering för att skydda mot obehörig läsning eller manipulation. Det finns flera produkter och tekniker för att uppnå skydd mot insyn och manipulation.
- Åtkomstskydd ska inte baseras på det ordinarie systemet för identitets- och åtkomsthantering (IAM) om det dessutom används för att säkerhetskopiera det ordinarie systemet för IAM. Detta leder till ett cirkulärt beroende.
- Åtkomstskyddet bör omfatta krav på fysisk närvaro och användning av en dedikerad klient. Åtkomst via virtuellt privat nätverk (VPN) bör inte tillåtas.
- Starka lösenord och återställningsrutiner bör förvaras på papper i ett säkerhetsskåp eller annan lämplig rutin.
- Nätverket bör vara segmenterat så att produktionsnätet och nätet för säkerhetskopior är åtskilda i olika zoner.
- Övervakningen av nätverket bör även omfatta den zon där säkerhetskopior lagras.

### 3.2.3 Utkontrakterade tjänster (Moln)

Om myndigheten gör bedömningen att det finns hinder för att lägga systemets drift i en molntjänst, så föreligger sannolikt samma hinder för att förvara säkerhetskopior i en molntjänst. Precis som när myndigheters nyttjande av molntjänster ibland blir möjliga via olika mitigerande åtgärder, så kan under vissa omständigheter även säkerhetskopiering lagras i molnet med vissa mitigerande åtgärder.

I bilaga 2, *Säkerhetskrav vid utkontraktering av it-tjänster,* står mer om krav vid upphandling av en utkontrakterad tjänst.

## 3.3 Segmentering

För att försvåra för en angripare att fritt röra sig inom myndighetens it-miljön är det rekommenderat att införa smarta segmenteringar inom it-landskapet. Detta kan vara dedikerade men logiskt separerade nätverk där övervakning sker på trafikflöden och användarbeteende. Trafik mellan resurser ska begränsas så att endas nödvändig trafik tillåts. Är kraven högre ställda t.ex. kring säkerhetsskyddad information, kan en fysisk segmentering behövas där information måste flyttas fysiskt enligt en beslutad arbetsprocess. Separation kan göras för olika typer av klienter, olika verksamheter inom myndigheten och olika typer av utrustning.

Segmentering bör användas för att minimera potentiell skada i it-landskapet men också för att skydda it-resurser (backuper, behörighetssystem, management, övervakning) som behövs vid en it-attack.

För ett ännu högre skydd kan en typ av "zero trust lösning"[11] införas för separation, där rätt roll, rätt geografiska plats, rätt valda enheter och i rätt tid får behörighet att utföra en viss typ av arbete med viss typ av informationmängd. Detta är rekommenderat för myndigheter som anser sig ha högre säkerhetskrav. Zero trust kan bestå av flera olika tekniker och kan ta tid att införa.

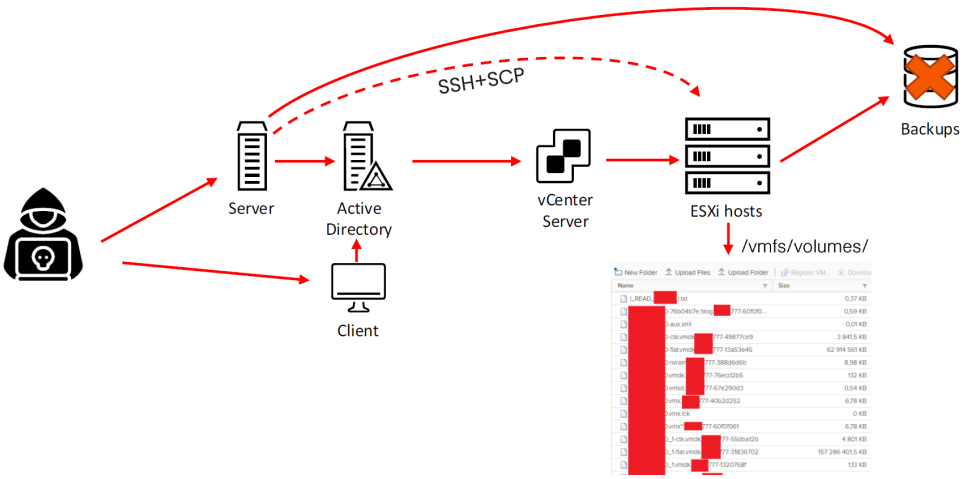
Det är även allmänt rekommenderat att myndigheten jobbar med separata administratörsdatorer så att systemadministrativa inloggningar inte sker från ordinarie arbetsstationer. Se exempelvis Microsofts koncept kallat privileged access workstation (PAW)[12].

## 3.4 Hypervisor

Hypervisor-plattformar[13] är ett annat högt prioriterat mål vid en ransomware-attack. Antagonisten försöker då få kontroll över hypervisor-miljön så att organisationen stängs ute från all egen access. När de virtuella servrarna och klienterna startas om efter en sådan attack,, är de fullt smittade och krypterade. Moderna hypervisors har visst skydd mot ransomware, t.ex. *säker uppstart* och *vitlista över godkänd exekverbar kod*, varför det är rekommenderat att de är påslagna och används.

[11] https://en.wikipedia.org/wiki/Zero_trust_security_model
[12] https://learn.microsoft.com/sv-se/shows/taste-of-premier/paws
[13] https://en.wikipedia.org/wiki/Hypervisor

### vSphere attackvektor




*Figur 2,* visar flödet i hur en ransomware attack mot Vmware övergripande kan ske i steg. Något som skiljer lite åt från varje attack. Källa Truesec.

eSams arbetsgrupp har fått en lista på åtgärder för att skydda sin hypervisor-miljö, av en svensk säkerhetsleverantör. Punktlistan ska ses som en inspiration och gör inte anspråk på att vara heltäckande:

- Skydda säkerhetskopior så att de inte kan skadas, även om hela produktionsmiljön görs otillgänglig.
- Segmentera hypervisor-miljö från övrig servermiljö och klienter
- Segmentera så att hypervisor-miljö och AD/katalogtjänst är åtskilda.
- Använd EDR/XDR/SIEM[14], för end point mot klienter och servrar.
- Tillämpa lämplig Managed Detection and Response (MDR)[15] alt Network Detection and Response (NDR).
- Installera regelbundet säkerhetsuppdateringar.
- God lösenordskultur med starka lösenord eller PAM[16].
- Härda hypervisorn enligt leverantörens guider.
- Använd vitlistning av kod för tillåten och godkänd exekverbar kod i hypervisorn.
- Hindra lateral[17] förflyttning mellan managementverktyg och plattform.

## 3.5 Säkerhetspatchning och sårbarhetsskanning

Attackvektorer för ransomware skapas ofta genom att utnyttja sårbara programvarukomponenter. För att undvika sårbarheter i system behöver systemen

[14] Förklaring; https://www.forbes.com/sites/forbestechcouncil/2021/04/15/edr-xdr-and-mdr-understanding-the-differences-behind-the-acronyms/
[15] Förklaring; https://www.orangecyberdefense.com/se/kunskap/faktablad/managed-detection-and-response
[16] Förklaring; https://en.wikipedia.org/wiki/Privileged_access_management
[17] Förklaring; https://www.cloudflare.com/learning/security/glossary/what-is-lateral-movement/

underhållas och säkerhetsuppdateringar läggas på så snart som möjligt efter att de släppts. Det är också viktigt att myndigheten håller sig uppdaterad med information från leverantörer när nya säkerhetsuppdateringar släpps. Cert-se publicerar löpande information om allvarliga sårbarheter och har en automatisk tjänst (ANTS[18]) för notifiering av tekniska sårbarheter som är exponerade mot internet.

Myndigheten behöver använda en kombination av verktyg och processer för ändamålet och säkerställa en aktiv sårbarhetsbevakning via skanning. Det är också viktigt att hålla sig uppdaterad på information från cybersäkerhetsmyndigheter. Mjukvara som nått End of life (EOL) får inte längre säkehetsuppdateringar och ska inte användas. Det är viktigt att tidigt identifiera vilka komponenter som går end of life så att det i systemens livscykelhantering så att det i god tid kan planeras för att byta ut komponenterna. Mjukvara som nått EOL status, bör minst hanteras som en kritisk sårbarhet. Om det inte är möjligt att avveckla/uppdatera mjukvaran, ska den segmenteras i ett separat nätverk för att undvika att den ”smittar” övrig it-miljö. Observera att icke-supporterad mjukvara måste ses som en absolut sista utväg och under planerad avveckling.

Patchning, dvs. installation av säkerhetsuppdateringar, ska ske löpande. En tidigare rekommandation har varit att installera säkerhetsuppdateringar inom 30 dagar från dagen då de släpps[19]. Idag bör ledtiderna för uppdateringar vara kortare. En metod kan vara att prioritera känsligare system eller kritiska sårbarheter, där myndigheten har en snabbare cykel. Vidare bör typen av exponering mot IT systemet påverka ett skyndsamt uppdateringsschema t.ex. externt exponerade IT system kontra system i låsta IT miljöer (utan publik access).

Organisationens kända sårbarheter bör beskrivas systematiskt. Gäller så väl hård- och mjukvara som rutiner och arbetssätt. Syftet bör vara att skapa en förteckning över alla negativa tillstånd som genom åtgärder kan förbättras eller elimineras. Arbetssättet bör integreras i befintliga strukturer för arbete i projekt och förvaltning.

Sammanställningen av myndighetens sårbarheter, bör av myndigheten tilldelas en hög skyddsnivå (hög sekretess alternativt säkerhetsskyddad information) för det fall att myndighetens sårbarhetskartläggningen kommer i fel händer. En sådan känlig information kan nyttjas vid angrepp eller sabotage.

Det är en rekommendation att myndigheter använder en sårbarhetsscanner som en del i arbetet med sårbarhetshantering. Behovet av uppdateringar bör normalt sett upptäckas och hanteras inom ramen för ordinarie systemförvaltning. Att använda sig av en

[18] Förklarande information; https://www.cert.se/rad-och-stod/ants/
[19] NIST Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology. Länk

sårbarhetsscanner ska endast betraktas som ett ”skyddsnät” för att upptäcka system där den ordinarie sårbarhetshanteringen inte fungerar. Sårbarhetsscannern kan hjälpa myndigheten att övergripande kartlägga och undersöka alla nätverksprotokoll/portar och i vissa fall utforska svagheter i applikationer.

En sårbarhetsscanner kan konfigureras att arbeta "mjukt", och endast kartlägga, vilket motsvarar s.k. port scanning. Mer avancerade verktyg kan gå längre och utföra mer invasiva eller rentav destruktiva operationer och blir då en automatiserad men enklare typ av manuell penetrationstestning. Det finns ett flertal produkter och tjänster med fri licens att välja mellan för sårbarhetsskanning.

Införande av sårbarhetsskanner introducerar ett informationssäkerhetsproblem, då alla funna sårbarheter måste hanteras som mycket känsliga och även under sekretess (enligt Offentlighets- och sekretesslag (2009:400) 18 kap 8§)[20]. Det betyder att myndigheten måste hantera denna informationsmängd där efter.

## 3.6 Provisionering och funktionsminimering

När myndigheten fångar upp ett sårbarhetslarm behövs en snabb bedömning i följande steg:

- Identifiera berörd systemkomponent.
- Samverka med it-säkerhetsfunktion och berörda drifts- eller förvaltningsorganisationer.
- Gör riskbedömning och eskalera beslut vid behov.
- Planera åtgärd, helst i formell change-process[21].
- Följ upp enligt gällande rutiner

Rutiner och systemstöd för provisionering (it- automatisering) av programvara bör vara tillgängliga liksom ett beskrivet och implementerat förändringsflöde.

Verktyg för säkerhetsautomation kallas för Security orchestration, automation and response (SOAR)[22]. Denna typ av samlingsverktyg kan vara kritiskt viktiga dels för snabb automatiserad respons för att undvika attack eller minimera skada av en uppstart av en ransomware attack. SOAR verktyg kan även automatisera planerade åtgärder för snabbare inövad manuellt initierad respons vid ett misstänkt angrepp för att undersöka eller begränsa attack.

[20] Offentlighets- och sekretesslag (2009:400). Länk
[21] https://onbird.se/grunderna-i-change/
[22] Föklaring begrepp; https://en.wikipedia.org/wiki/Security_orchestration

Myndigheter bör slå av it funktioner som inte används för att minska tänkbar attackvägar. Precis som standardklienter bör myndigheter ha standard serverroller med enbart rätt funktioner aktiverade alernativt contanterlösningar med liknande säkerhetkonfiguration.

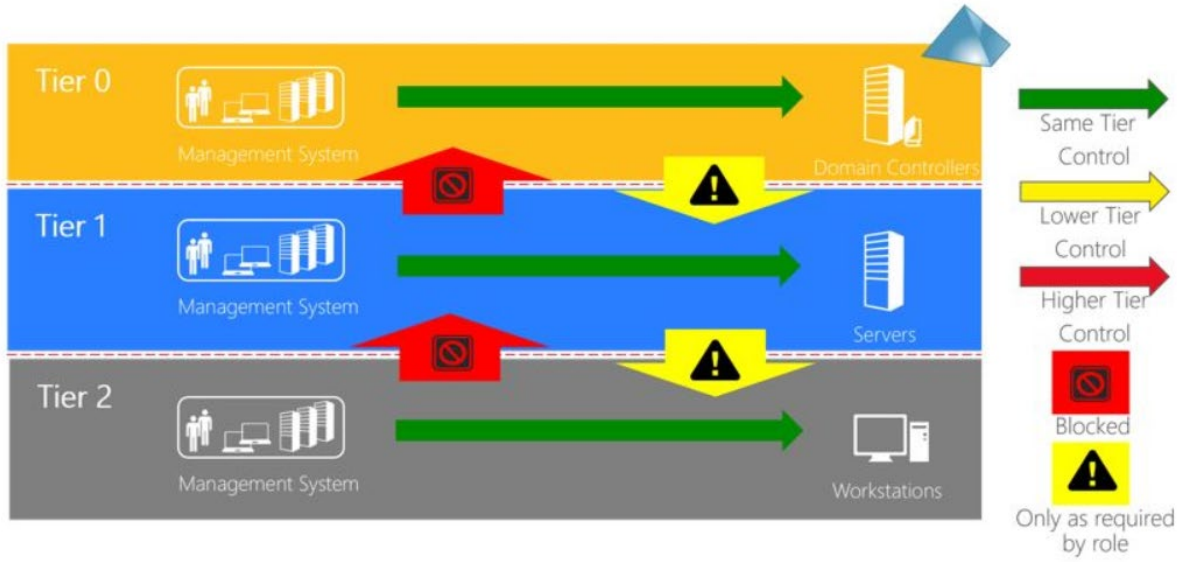
## 3.7 Separera behörighetssystem (PAM)

I inledningen av en ransomware-attack försöker antagonisten ofta få kontroll över organisationens katalogtjänst (Active directory) och dess administratörskonton. Därmed är detta en kritiskt viktig resurs att övervaka vad gäller oplanerade ändringar, t.ex. ändrade lösenord för administratörskonton, nya tillkommande administratörskonton och borttagande av administratörskonton.

Det är rekommenderat att myndigheter har en skiktning (teiring) av sin katalogtjänst ur ett lämpligt säkerhetsperspektiv. För högre säkerhetskrav hos myndigheten rekommenderas Privileged Access Management - PAM[23] och priviligierade managementstationer - PAW-lösningar, just-in-time (JIT)[24] och/eller Zerotrust ticket access för åtkomst till it-resurser istället för traditionell konto/token autentisering. Använd kontoseparering för att undvika att ett konto används till alla arbetsuppgifter och mot alla it-lösningar. Det är även önskvärt att myndigheten tar fram en egen modell för tiering[25] av katalogtjänst.

Ännu en rekommendation är att t.ex. dela upp olika administrativa arbetsuppgifter med segmenterade adminklienter då både klienter och användare ofta kan vara utpekade mål för en attack mot myndigheten. Konton och klienter bör exponeras minimalt, vilket går väl ihop med tier-konceptet av katalogtjänst enligt bilden nedan där där en admin-klient kan segmenteras till viss nivå i katalogtjänstens säkerhetsstruktur och inloggning kan styras för varje administrativ arbetsuppgift till rätt säkerhetsnivå.

[23] https://en.wikipedia.org/wiki/Privileged_access_management
[24] https://www.cyberark.com/what-is/just-in-time-access/
[25] https://www.truesec.com/security/active-directory-tiering




*Active Directory Tiered Administrative Model Control Restrictions (Image Credit: Microsoft)*

*Figur 3, visar övergripande PAM och PAW koncept bidrar praktiskt till effektivare skydd från ransomware genom separation i olika led. Källa Microsoft.*

## 3.8 Säkerhetskultur

En god säkerhetskultur är en framgångsfaktor för att minimera ransomware-attacker. För att skapa medvetenhet och vaksamhet i organisationen i syfte att minimera attacker mot myndigheten, bör det finnas beslutade riktlinjer och olika former av stöd till medarbetare. Det är viktigt att alla känner till vad som är rätt beteenden och riktiga val.

Myndigheten för samhällsskydd och beredskap nämner särskilt arbetet med systemägarskap, som ett krav för myndigheter i MSBFS 2020:7 2 kap 1§. Systemägarskap innebär att det ska finnas en utpekad roll i myndigheten, som ansvarar för att införa, följa upp och utreda skyddet i enskilda it-lösningar och it-miljöer som en viktig del i en god säkerhetskultur.

Ett sätt att bygga en säkerhetskultur brett inom organisationen kan vara att berätta om olika typer av risker och incidenter. Ett stödjande och coachande förhållningssätt ökar sannolikheten för att bygga en stark säkerhetskultur. Det finns inga hundraprocentiga skydd mot riktade attacker, men organisationen ska vara motiverad att göra det svårt för en angripare i så stor utsträckning som möjligt.

## 3.9 Hot-modellering

Vid hot-modellering beskriver organisationen några scenarion om hur en aktör kan bete sig för att få in den skadliga koden i it-miljön. Därefter identifierar myndigheten vilka

steg i ett angrepp som kan avvärjas på det mest kostnadseffektiva sättet. Det här kan vara ett bra sätt att bygga upp en förståelse för ramsomeware-angrepp i organisationen.

## 3.10 Leverantörer/Partners

Myndigheten behöver ställa krav på dels hur leverantörer ska larma myndigheten om leverantören drabbas av skadlig kod, dels att ha en handlingsplan för hur myndigheten ska agera om det inträffar. Handlingsplanen bör t.ex. innehålla instruktioner om viss trafik ska stängas mot leverantören, vilka rutiner som ska sättas igång internt och vilka omständigheter som ska föreligga för att myndigheten kan besluta om att öppna upp trafik till leverantören på nytt.

Kraven myndigheter behöver ställa bör också omfatta underleverantörer för att säkra hela leverantörskedjan. För mer detaljerade krav hänvisas till kommande lagkrav utifrån NIS2/CER EU direktiven.

## 3.11 Övning

Alla myndigheter som själv bedömmer att man omfattas av beredskapsförordningen (2022:524)[26] ska genomföra kvartalsvisa kris- och beredskapsövningar, men övningsverksamhet är användbart för alla organisationer. Förmågan att hantera allvarliga it-incidenter är naturliga delar i sådan övningsverksamhet, men övningar kan utsträckas till många andra områden. Övningar kräver både planering och resurstilldelning och kan vara krävande för organisationer som tidigare inte har prioriterat detta. Flera viktiga beslut behöver fattas som t.ex. om övningarna ska genomföras lokalt i olika arbetsgrupper eller om aktiviteterna ska samordnas i större övningar.

På området it-säkerhet kan organisationen genomföra övningar som antingen attack eller försvarsövningar (Red Team/Blue Team[27]) eller som ledningsövningar. Kombinationer av dessa går också bra. Övningarna bör planeras noga. Identifiera de övande funktionerna, ha en tydlig ledning och se till att de leder till tydliga rapporter. Identifierade brister bör dokumenteras oavsett om bristerna är av teknisk natur eller rör arbetssätt och rutiner. Rutinerna för rapportering av övningar bör vara snarlika de som används för incidenter.

Övning ger trygghet och verifierar att återställningsplanen är korrekt samt att de olika systemens återställning samverkar med varandra. Säkerställ att planen håller som det är

[26] Förordning (2022:524) om statliga myndigheters beredskap. Länk
[27] Förklaring av begrepp; https://dizparc.se/inspiration/red-team-vs-blue-team-vi-reder-ut

tänkt och att utpekade roller och ansvariga är korrekt. En återställningsplan kan betraktas som färdig först när den verifierats i en övning.

Genom övning verifieras även säkerhetskopior och system för hantering av säkerhetskopior. Kvartalsvisa övningar bibehåller kompetens och förmåga och ger följsamhet mot föreskrifter från MSB och beredskapsförordningen.

Myndigheten bör ta med leverantörer i övningarna.

# 4. Upptäcka

Förmågan att snabbt upptäcka ett angrepp är en förutsättning för att kunna stoppa eller begränsa attacken.

## 4.1 Security Operations Center - SOC och Security Information and Event Management - SIEM.

En SOC arbetar både med loggar och larm. Loggar analyserar kontinuerligt för att identifiera avvikelser och förbättra den övergripande säkerheten. Larm triggar direkta undersökningar och åtgärder för att snabbt svara på hot eller misstänkt aktivitet. En effektiv SOC kombinerar alltså logganalys och larmrespons för att både upptäcka och hantera potentiella säkerhetshot i realtid.

För att en organisation ska ha förmåga att se vad som händer i systemen under en attack eller vad som hänt i systemen fram till dess att organisationen upptäckt en attack, bör systemen för it-managering vara skyddade och separerade från produktionsmiljön. Detta kan omfatta system som EDR, övervakning och distributions- eller manageringsverktyg som organisationer behöver för att återställa miljön och utreda vad som har hänt, samt vid en eventuell forensisk analys.

Det är ett krav att myndigheter kan hantera behörigheter och har förmåga till snabb hantering när oväntade förändringar görs i dessa verktyg.[28].

En SOC[29]-funktion kan ha många olika namn. I den här rapporten definieras begreppet som en samling av följande:

[28] MSBFS 2020:7 kap 4 §16, 17, 18, 19
[29] https://www.techtarget.com/searchsecurity/tip/CERT-vs-CSIRT-vs-SOC-Whats-the-difference

- Förmåga att utreda vad antagonisten utfört i it-miljön och vid en forensisk analys.
- Förmågan att läsa loggar och upptäcka anomalier, gärna maskinellt och gärna i realtid eller realtidsnära.
- Förmåga till sårbarhetsskanning av de egna systemen.
- Förmåga att skanna internet efter spår som avslöjar angriparen, t.ex. på sociala medier, i chattforum och på webbplatser där antagonister sprider kunskap om nya sårbarheter och skryter om olika it-angrepp.

Det är önskvärt att alla myndigheter har en e-postadress; soc at myndighet.se för att enkelt kunna kontakta varandra.

Upptäckter som SOC-funktionen gör, behöver kopplas till organisationens incidenthanteringsprocess där händelsen dokumenteras, utreds, eskaleras och åtgärdas. Det är viktigt att olika typer av incidenter ingår eftersom en incident kan övergå i en annan eller pågå parallellt; tex driftincident, it-säkerhet, informationssäkerhetsincident, säkerhetsskyddsincident, fysisk säkerhet, personuppgiftsincident, personalsäkerhet etc. Baserat på att olika incidenter ska rapporteras till olika myndigheter baserat på dess karaktär MSB, Säkerhetspolisen, Integritetsskyddsmyndigheten (IMY) behöver även denna aspekt beaktas vid incidenthanteringsarbetet. Organisationen behöver definiera vilka mandat som är kopplade till SOC-funktionen och incidenthanteringsprocessen och föra in detta i ett ledningssystem (LIS).

SOC, incidenthantering och problemhantering behöver knytas ihop till en stor övergripande process med smidiga flöden mellan delprocesserna. Eftersom det är en längre process att bygga upp en SOC-funktion är det lättast att upphandla funktionen på marknaden. Nackdelen med detta är att myndigheten då behöver lämna ut mycket känslig information och behörigheter till en extern part vilket i sig kan vara problematiskt (säkerhetsmässigt och juridiskt). Målet bör vara att på sikt kunna bemanna en SOC med egen personal för att övervaka händelseloggar för de egna systemen. För myndigheter med få resurser kan myndigheten börja i en liten skala där myndigheten kanske bara bemannar kontorstid med egen personal samtidigt som myndigheten har en extern part som täcker upp dygnets övriga timmar.

Arbetsuppgifterna kan skäras på andra sätt, exempelvis kan myndigheten ha en första linje och en andra linje support. En sådan lösning har fördelen att personalen specialiseras och bygger spetskompetens i den andra linjen, medan nackdelen kan vara att den första linjen inte upplevs vara lika utvecklande och kan leda till en högre personalomsättning.

För myndigheter som eventuellt saknar förmåga för SOC är en rekommenderad startpunkt att först investera i EDR och SIEM. Över tid kan myndigheten skapa en SOC förmåga.

### 4.1.1 Att upphandla SOC

Vid upphandling av ett Security operations center, behöver myndigheten ta ställning till samma frågor som när den byggs upp i egen regi. Arbetsgruppen hänvisar till eSam ”Vägledning utkontraktering – sekretess och dataskydd”[30] som stöd vid anskaffning av denna tjänst. Som kravställare behöver man förstå och dokumentera behov för vilka aktivitetsnivåer som larm ska aktiveras och vilka övervakningsfall som behöver bevakning. Som beställare ansvarar man för att informera leverantören om myndighetens prioritering av olika system och hur larm och förslag på motåtgärder ska eskaleras för beslut.

Finns det ett incidentrespons-team så behöver det kopplas ihop med SOC-funktionen, om inte kan myndigheten även behöva upphandla detta.

### 4.1.2 Övervakning av externa it-tjänster

Myndigheten behöver ha en strategi för övervakning och kravställa mot den vid upphandling av it-tjänster. Skälet är att när it-tjänster driftas externt, kan det vara svårt att förse systemet för logganalys med information från en extern part. Ibland tillhandahålls webbgränssnitt för att granska loggar, men en sådan lösning kan vara svår att integrera i informationsflödet i en SOC. Ett par gränssnitt kan i allmänhet hanteras men övervakningen blir ineffektiv och kostsam om det blir väldigt många olika it tjänster.

Trots att många tjänsteleverantörer tillhandahåller ett API för automatiserad koppling till ett eget system för övervakning, så kan stora mängder integrationer göra övervakningen ineffektiv.

### 4.1.3 Drift

Drift av system för SOC kan för vissa myndigheter behöva upphandlas då det är många loggar som behöver läsas in i systemet. Något som kan bli problematiskt då skyddsvärdet kan öka av den aggregerade informationsmängden. Utländska molntjänster kan vara

[30] Vägledning; https://www.esamverka.se/download/18.43a3add4188b9f2345a2fe78/1687332814480/ES2023-06%20V%C3%A4gledning%20Utkontraktering%20-%20sekretess%20och%20dataskydd.pdf

olämpliga på grund av den stora mängden insamlad information som medför att tjänsten kartlägger användarnas beteenden.

Metoden för övervakning är att ett stort antal loggfiler läses in i ett system och analyseras realtidsnära för att upptäcka misstänkt felaktig användning eller avvikande användarbeteende. En väl integrerad lösning med automatiserad inläsning av detaljerade loggar, ger ett bättre underlag för att upptäcka intrång eller felaktig användning, samtidigt som myndigheten också behöver beakta andra relaterade krav tex att värna om användarnas integritet.

### 4.1.4 Omvärldsbevakning

För att kunna bedriva ett operativt it-säkerhetsarbete med god framförhållning, är det viktigt att på daglig basis följa aktuella händelser i omvärlden, i synnerhet hotrörelser och allvarliga sårbarheter. Det finns flera källor med möjlighet att prenumerera på bransch-nyheter, t.ex. hos CERT-SE, NCSC.gov.uk och CISA.gov men såklart även vanliga nyhetskanaler och sociala medie-plattformar. Ännu ett sätt att hålla sig uppdaterad är genom digitala verktyg för inhämtning av hotunderrättelser och andra signaler.

### 4.1.5 Bemanning och beredskap

Angrepp och incidenter kan inträffa när som helst och det kan av olika skäl vara svårt att bemanna en funktion dygnet runt.

En kompromiss kan vara att ha egen personal kontorstid och en upphandlad tjänst utanför kontorstid eller automatiserade larm med beredskap för inställelse av egen personal. Det viktiga är att göra en medveten prioritering av bemanningen.

En incident eller ett angrepp kan pågå i flera dagar eller ännu längre och det är viktigt att prioritera de personella resurserna för att undvika att medarbetare behöver gå hem för dygnsvila vid samma tidpunkt. Ta inte alla resurser i anspråk omedelbart utan planera så att medarbetarna kan byta av varandra.

### 4.1.6 Mandat

SOC-funktionen behöver ha ett väl avvägt mandat för att kunna agera vid misstanke om angrepp. Det behövs  en rutin för när system får stängas ner. Av rutinen behöver t.ex. framgå vilka beslutsfattare som ska kallas in och hur myndigheten ska hantera en situation där man inte får tag i rätt beslutsfattare i ett akutläge.

I fasen *Begränsa* (kapitel 5.4) kan frågan om mandat lätt bli en fördröjande faktor. Det är en fördel om myndigheten i förväg har diskuterat frågan om vem som kan koppla bort/ta ner ett system, på vilka grunder och hur länge. Ett långtgående mandat ger bättre möjlighet till skyndsam och effektiv hantering. En uppföljning och ett ansvarsutkrävande kan hanteras efter incidenten.

# 5. Åtgärda ransomware

Om ransomware eller skadlig kod drabbar organisationen så upptäcks det huvudsakligen på tre sätt:

- Via ett security operations center -SOC (se kapitlet 4.1)
- Via en användare som rapporterar en incident
- Via it-driften som rapporterar en incident

Oavsett hur det går till, ska organisationen upprätta en incidentrapport och initiera den ordinarie incidentprocessen. Det finns alltid en risk för att incidenten kan medföra en väldigt stor påverkan på verksamheten varför den behöver hanteras skyndsamt och bör klassificeras som en kritisk incident. Den eventuella skuldfrågan är sekundär i det här läget.

## 5.1 Incident och Response team

Organisationen behöver ha ett avdelat och bemannat incidentrespons-team. Det kan vara egen personal eller konsulter. Förutom kontaktvägar och inställelsetid behöver teamet kunna byta bemanning för vila under längre incidenter. Vid en incident behöver organisationen aktivera sin krisstab för att dels hantera den interna och externa kommunikationen om incidenten, dels kunna utreda handlingsalternativ för att lägga om verksamheten eller aktivera reservrutiner.

## 5.2 Säkerhetslogg och säkra spår

Under en pågående incident med hög stressnivå och krav på skyndsamhet, behöver myndigheten ha förmåga att samla in och sammanställa forensiska spår och bevismaterial i en säkerhetslogg. Det är viktigt att prioritera detta trots hög belastning eftersom det är viktigt för incidentrapporteringen och eventuell rapportering till andra myndigheter. Det finns krav på detta i MSB-FS 2020:8[31] och beroende på vilken typ av incident som inträffat, kan myndigheten behöva rapportera till fler tillsynsmyndigheter.

[31] MSB föreskrifter om rapportering av it-incidenter för statliga myndigheter paragraf 2. Länk

När den skadliga koden tas bort behöver myndigheten säkra bevis och spår i form av loggar.

Har teamet identifierat angreppssättet, eller i alla fall har starka teorier kring hur det gått till, så ska säkerhetshöjande åtgärder implementeras för att angreppet inte ska återkomma på samma sätt.

## 5.3 Analysera

Myndigheten behöver identifiera vilka tjänster, enheter eller användare som kan vara utsatta och snabbt upprätta en första lägesbild (kan även kallas konsekvensanalys) av händelsen. Analysen behöver därefter itereras och uppdateras under hela incidenten. Myndigheten behöver också fastställa när och hur den skadliga koden tog sig in i systemen.

Det är viktigt att säkra olika typer av spår, exempelvis loggar, som bevismaterial. Vissa loggar kan ha kort rotationstid, så det kan vara taktiskt att några arbetar med att samla in alla loggar medan andra jobbar med att analysera loggarna.

Tidigt under incidenten och sedan löpande under arbetets gång, behöver myndigheter som Integritetsskyddsmyndigheten[32] och Myndigheten för samhällsskydd och beredskap[33], uppdateras med en rapport som slutligt kompletteras när incidenten är hanterad och avslutad.

Aktiviteter i fasen *Begränsa (kapitel 5.4)* behöver påbörjas skyndsamt. Därför är det viktigt att den första versionen av analysen är klar tidigt men ändå kan ge en tillräckligt bra lägesbild. Både faserna *Analysera* och *Begränsa* itereras i väldigt korta iterationer.

### 5.3.1 Hitta källan och tidpunkten

När källan väl är hittad och spridningen kartlagd och begränsad, så avslutas de föregående faserna och hanteringen övergår i en ny fas.

Parallellt med att faserna *Analysera* och *Begränsa* pågår, kan angriparen presentera krav på en lösensumma. Enligt cert.se ska lösen aldrig betalas ut [34].

Det kan också vara bra att på förhand ha utsett en förhandlare som är tränad inför en förhandlingssituation.

[32] https://www.imy.se/verksamhet/utfora-arenden/anmal-personuppgiftsincident/
[33] https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/hantera-och-rapportera-it-incidenter-och-cyberangrepp/rapportera-it-incident/statlig-myndighet---rapportera-it-incident/
[34] https://cert.se/tema/ransomware/

## 5.4 Begränsa

Utifrån vad som är känt behöver myndigheten isolera de infekterade/angripna systemen, koppla bort system ifrån varandra, byta lösenord på vissa konton, stänga av vissa konton, skärma av så långt som möjligt och blockera attackvektorer. Ett tips är att myndigheten kan sätta upp och använda VPN för att styra, begränsa och isolera attacken. Det kan röra sig om att stänga ner löneutbetalningsfunktionen om löneutbetalningen inte är tänkt att gå just den här dagen eller att stänga e-tjänster som inte måste hållas öppna. Kan användare eller sammankopplade system till det angripna systemet kopplas bort, så bidrar det till att isolera angreppet.

## 5.5 Planer för olika scenarion

Det är rekommenderat att myndigheten vid behov har flera planer för olika scenarion kring skadlig kod och att de tas fram skyndsamt så att de finns på plats innan en incident inträffar.

Rätt planen aktiveras i processen när en *Major incident*[35] identifierats då en incidentledare får en notis om att den har inträffat och kan aktivera *incidentresponsteamet.*

### 5.5.1 Bemanningsplan

Myndigheten behöver kunna bemanna flera team (egna eller hos leverantör hos upphandlad tjänst) som kan tjänstgöra i skift i enlighet med bemanningsplan. Planera även för överlämning mellan teamen.

Myndigheten ska ha utsett förutbestämda primära digitala och analoga kanaler samt kontakt för beslutsfattare i tjänst. Planera för att kunna lösa av incidentledare och responsteam. Identifiera nyckelpersoner som är kritiska för hantering för olika typer av incidenter. Organisera ett responsteam med en kommunikatör som hanterar kommunikationen utåt. Även inom gruppen är det viktigt att hålla professionell ton och god kommunikation. Planera gärna även för en mat- och fikaansvarig som även påminner om raster och när folk behöver gå hem för att vila. Framtagandet av en bemanningsplan medför sannolikt arbetsrättsliga frågor av olika slag. Den typen av frågor tar ofta tid att reda ut och behöver hanteras tillsammans med myndighetens personalfunktion. Er bemanningsplan bör omfatta följande delar på utskrivet papper:

- Bemanningsplanen ska innehålla kontaktuppgifter till alla ingående personer och roller.

[35] Myndigheter definierar själva sina nivåer för incidenter och nycklar för eskalering till en ”major incident”. Generellt ITIL definition ”major incident”; https://advisera.com/20000academy/knowledgebase/major-incident-management-going-gets-tough/

- Planen ska också innehålla beslutade kontaktrutiner.
- Ett responsteam behöver finnas, bestående av egen personal eller via leverantör. Bemanningen bör vara förberedd för att arbeta i skift med en överbemanning så att några kan vila medan andra arbetar. Jouravtal kan behövas med avtalad inställelsetid.
- Logganalytiker och erfarna utredare behöver ingå i teamet
- Övergripande arkitektonisk kunskap behöver finnas med kunskap om vilka system som bidrar till vilka verksamheter för att kunna bedöma verksamhetskonsekvenser
- Beslutsfattare kan behöva samlas i en krisledning.
- Kommunikatörer behöver kunna informera internt och externt.
- HR-frågor, medarbetare inblandad i händelsen
- En förhandlare bör vara utsedd med utbildning och strategier planerade i förväg
- Behörighetsadministratörer behöver finnas tillgängliga under incidenten
- Tekniker som handhar och kan återställa backuper behövs
- Även under en Major incident och krissituation[36] behöver myndigheten ha en god arbetsmiljö. Praktikaliteter kring inpassering och mat behöver fungera för anställda och konsulter under de tider man arbetar.

### 5.5.2 Eskaleringsplan

Organisationen behöver en eskaleringsplan för att eskalering kan göras i rätt tid, smidigt och med god kvalitet. Eskalering och de-eskalering bör övas och ske efter fördefinierade tröskelvärden eller milstolpar.

Från ett normalläge behöver myndigheten kunna gå upp i incidentläge och krisläge för att sedan de-eskalera tillbaka till normalläget.

### 5.5.3 Kommunikationsplan

Vid en incident är kommunikationen med de som berörs av den, viktig. Det kan t.ex. handla om externa tjänster som påverkas, varför information behöver gå ut så snart organisationen har bildat sig en uppfattning av situationen. Incidentteamet och kommunikationsavdelningen behöver snabbt sätta upp en grupp för både extern och intern kommunikation. Initialt är det viktigt att identifiera vilka grupper som berörs av händelsen, formulera 3 - 4 tydliga budskap, utse en talesperson och kommunicera i

[36] https://www.msb.se/sv/amnesomraden/skolmaterial/samhallets-krisberedskap/vad-ar-en-kris/

kanaler som når de berörda i den aktuella situationen. Det kan variera från incident till incident, varför man inte kan fastställa **ett** tillvägagångssätt. Det beror på vad som hänt.

Planera kommunikationstillfällen så att de som arbetar med att hantera incidenten, får arbetsro, en talesperson som står utanför den gruppen är därför att föredra. Håll myndighetens ledningsgrupp löpande informerad.

Om den externa webbplatsen går ner, behövs en nöd-webb som driftas utanför den ordinarie it-miljön. Där bör de viktigaste tjänsterna samt löpande uppdaterad information om incidenten prioriteras. Tänk också på att planera för och etablera analoga interna kommunikationsvägar i händelse av att de digitala interna kanalerna inte fungerar.

Det är viktigt att kommunikationsrutinerna är en del av organisationens incidentövningar så att de som blir berörda i skarpt läge är förberedda.

### 5.5.4 Återställningsplan

Om myndigheten behöver återställa system efter en incident, är det viktigt att ha återställningsplaner som alla känner till. Det skapar trygghet och gör att återställningen går smidigare. Det bör finnas planer både för att återställa system var för sig och som en helhet för det fall en fullständig återställning blir nödvändig.

I dokumentationen för varje system ska det framgå hur organisationen återläser och återstartar systemet och vilka andra system det finns beroenden till.

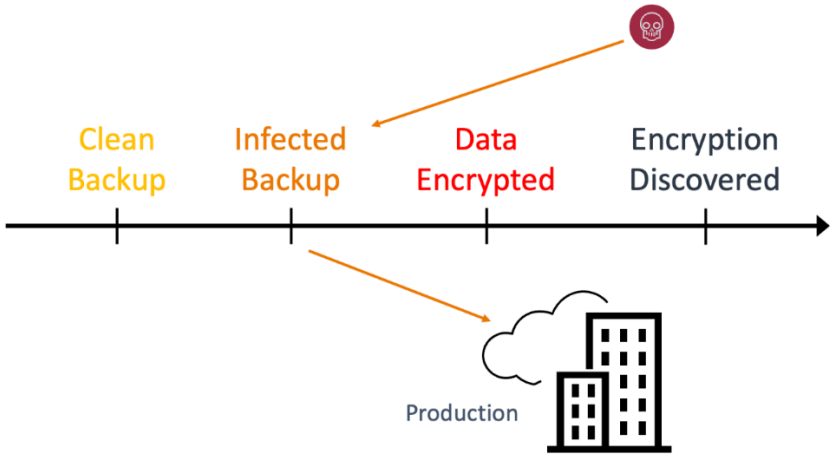
I en fullständig återställningsplan - Disaster Recovery Plan - ska det framgå i vilken ordning systemen ska återställas. Det är en fördel om aktuella konfigurationer är dokumenterade, det kan ge insikter om cirkulära beroenden som behöver lösas ut.

Myndigheten behöver också säkerställa att det finns en aktuell beroendekarta över alla driftkomponenter. Incident manager behöver en arkitekturbeskrivning i sammanfattad form som ett verktyg för att hantera incidenter.[37]

[37] https://www.msb.se/contentassets/af96031de7124f69a19fb936b78a478b/fspos-vagledning-for-kontinuitetshantering-version5.0.pdf

# 6. Återställa efter ransomware

Efter en incident behöver systemen återställas skyndsamt. Hur väl återställningsarbetet går, beror på kvaliteten på dokumentationen och den tid som verksamheten lagt på att öva. Genom att prioritera det förebyggande arbetet, ökar sannolikheten för att återställningarna går bra. Efter en incident är stressnivån ofta hög hos medarbetarna varför regelbundna övningar och en gedigen dokumentation är till stor hjälp för att genomföra återställningen under mindre press.




*Figur 4, Bilden visar balansen mellan att välja smittfri (clean backup) eller smittad backup (infected backup) vid återställning av attackerad It miljö, valet mellan riskfri återställning kontra behovet av återställning av myndighetens senaste informationsmängder. Döskallen visar när backuper smittas i tidsaxel. Källa VMware blogs.*

## 6.1 Återställa IT system

Oavsett om hela servern eller bara data återställs från backup, så behöver backuper kvalitetssäkras. Beroende på första kända datum för angreppet eller intrånget behöver verksamheten välja och verifiera en säker backup. Enligt myndighetens förebyggande arbete ska informationsmängder återställas enligt plan. Läs mer i kap *3.2.1 planering för säkerhetskopiering* om vilka förebyggande aktiviteterna som behöver göras.

Under återställningsfasen ska de säkerhetshål som antagonisten kan ha skapat eller utnyttjat till den smittade IT-miljön, säkras upp. Återställningen bör göras med stöd av god expertkompetens och med stödverktyg som EDR.

Förhoppningsvis har myndigheten tillgång till fungerande backuper vid en attack som ett resultat av att verksamheten har skapat säkerhetskopior med skydd mot manipulation och/eller har förvarat backuperna oåtkomligt för angripare. Rekommendationen är att

återsätta senaste fungerande backup i en kontrollerad och isolerad återställningsmiljö (även om den kan innehålla skadlig kod från tiden innan krypteringen aktiverades).

Vilka backuper man utgår ifrån att återställa, blir en svår bedömning för myndigheten. Har myndigheten hittat och täppt till sårbarhet och eventuella ”bakdörrar”[38][39] kring attacken? Med andra ord är dörren stängd mot antagonisten, även vid återställning av smittad backup? Vad är affärsvärdet för återställning till senaste backup (vikten för myndighetsuppdraget)? En smittad backup kan ändå återställas om myndigheten bedömer att verksamheten måste ha senaste backup återläst och man därmed kan säja att säkerhetshotet är hanterat.

## 6.2 Verifiera återställningen

Det är viktigt att verifiera att återställningen har gett önskad effekt och funktion. Se gärna till att ha flera verksamhetsrepresentanter vidtalade i förväg för att få snabb återkoppling. Om myndigheten har resurser att även använda automation för verifieringen är det ett bra komplement.

## 6.3 Utvärdera/Rapportera

Om det inte gjorts tidigare är det lämpligt att upprätta polisanmälan i samband med utvärderingen.

Sammanställ rapporteringen till IMY eller MSB och diarieför kommunikationen. Skapa ett ärende per incident där dokumentationen kring incidenten samlas. All extern kommunikation ska diarieföras i ärendet, till exempel polisanmälan och rapporter sammanställda till IMY, MSB eller andra myndigheter. Även internt material som rör incidenten bör diarieföras i ärendet, till exempel incidentrapporten och resultatet från utvärderingsarbetet. Om ärendet innehåller sekretessbelagda uppgifter ska det markeras så att ingen obehörig får tillgång till ärendet.

Myndigheten bör därefter genomföra en retrospektiv workshop i en förlåtande och lärande miljö kring vad myndigheten kunde ha gjort annorlunda och mer effektivt. Dokumentera lärdomar och insikter och uppdatera handlingsplan och bemanningsplan utifrån insikterna. Om det finns skäl kan även rollernas mandat och ansvar utvärderas.

Det är viktigt att utvärderings- och rapporteringsarbetet görs sammanhållet så att deltagarna kan överblicka all information från incidenten. Om det finns brister i

[38] https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cyber-attack/what-is-a-backdoor-attack/
[39] https://sv.wikipedia.org/wiki/Rootkit

ärendehantering och informationsdelning så blir det tydligt när det är dags för utvärdering och rapportering. Notera också att vissa inrapporteringsfunktioner, t.ex. från MSB[40] ställer krav på att det finns en rapportör som följer med under hela incidenten och som autentiseras med någon form av elektronisk ID-lösning.

# 7. Lärdomar

I incident-processen behöver myndigheten beskriva hur man ska arbeta med lärdomar och insikter som ska leda till kontinuerliga förbättringar. Medan en incident pågår dokumenteras händelser och aktiviteter i en händelselogg som är en viktig källa att gå tillbaka till när incidenten i efterhand ska beskrivas i en mer sammanfattad incidentrapport. Rapporten innehåller vanligtvis en analys där man identifierar grundorsaken till det som orsakat incidenten.

Två frågor som är bra att ställa:

- Vad kan vi göra för att minska sannolikheten att incidenten inträffar igen?
- Om incidenten inträffar igen, hur ska vi agera för att hantera incidenten mer effektivt?

Stödjande frågor i arbetet:

- Vad hade kunnat hända om förutsättningarna varit något sämre?
- Vilka var framgångsfaktorerna i hanteringen av incidenten?

## 7.1 Länktips

CERT.SE
https://cert.se/tema/ransomware/

NIST guide:
https://csrc.nist.gov/Projects/ransomware-protection-and-response

Storbritanniens nationella cybersäkerhetscenter:
https://www.ncsc.gov.uk/ransomware/home

MSB: Cyberangrepp mot samhällsviktiga informationssystem: 25 rekommendationer för stärkt skydd mot cyberangrepp
https://www.msb.se/sv/publikationer/cyberangrepp-mot-samhallsviktiga-informationssystem--25-rekommendationer-for-starkt-skydd-mot-cyberangrepp/

Följ leverantörens rekommendation kring konfiguration, vilket också nämns i MSBFS 2020:7 kap 3 § 1.

[40] https://www.msb.se/sv/regler/gallande-regler/krisberedskap-och-informationssakerhet/foreskrifter-om-rapportering-av-it-incidenter-for-statliga-myndigheter-msbfs-20208/

eSam är ett medlemsdrivet program för samverkan mellan myndigheter för att underlätta och påskynda digitaliseringen inom det offentliga. En viktig uppgift för eSam är att ta fram stöd och vägledningar som ger förutsättningar för att öka den digitala samverkan inom offentlig förvaltning.

Alla stöddokument finns på esamverka.se

I eSam ingår Arbetsförmedlingen, Arbetsmiljöverket, Bolagsverket, Boverket, Centrala Studiestödsnämnden, Domstolsverket, E-hälsomyndigheten, Ekonomistyrningsverket, Finansinspektionen, Folkhälsomyndigheten, Försäkringskassan, Havs- och vattenmyndigheten, Inspektionen för vård och omsorg, Jordbruksverket, Kemikalieinspektionen, Kriminalvården, Kronofogdemyndigheten, Kustbevakningen, Lantmäteriet, Livsmedelsverket, Länsstyrelserna, Migrationsverket, Naturvårdsverket, Pensionsmyndigheten, Riksantikvarieämbetet, Riksarkivet, Rättsmedicinalverket, Sida, Skatteverket, Skolverket, Statens institutionsstyrelse, Statens servicecenter, Statens tjänstepensionsverk, Statens veterinärmedicinska anstalt, Statistiska centralbyrån, Tillväxtverket, Trafikverket, Transportstyrelsen, Tullverket, Universitets- och högskolerådet samt Utbetalningsmyndigheten (juni 2024)