Myndigheten för samhällsskydd och beredskap

# Incidenthantering för **cyberfysiska system**

# Incidenthanteringsgruppens kontaktuppgifter

| |
|---|
| Namn: |
| Titel: |
| Tel. arbete: |
| Tel. mobil: |
| E-post: |
| Adress: |

| |
|---|
| Namn: |
| Titel: |
| Tel. arbete: |
| Tel. mobil: |
| E-post: |
| Adress: |

| |
|---|
| Namn: |
| Titel: |
| Tel. arbete: |
| Tel. mobil: |
| E-post: |
| Adress: |

| |
|---|
| Namn: |
| Titel: |
| Tel. arbete: |
| Tel. mobil: |
| E-post: |
| Adress: |

## Anteckningar, stöd för åtgärder i din verksamhet:

# Nu händer det saker, men vad har verkligen hänt?[1]

! Information om en potentiell incident inkommer från exempelvis säkerhetsprogram eller loggar, alternativt från medarbetare, kunder eller leverantörer.

1 **Sammankalla incidenthanteringsgruppen.** Ta ett steg tillbaka och analysera läget. Något har hänt eller något pågår – dags att hantera det!

2 **Detektera.** Vad vet vi och vilken information finns att tillgå? Varifrån kommer informationen? Var ska vi leta efter information som inte redan är given? Sammanställ den insamlade informationen och identifiera det kvarvarande informationsbehovet.

3 **Definiera.** Är det en incident? Är incidenten pågående? Vilken skada har skett? Vad kan eller kommer troligtvis att ske? Vilka system är påverkade?

4 **Sortera och prioritera.** Kontakta dem som behövs internt och externt. Informera berörda. Prioritera åtgärder. Ta beslut. Delegera arbetsuppgifter. Säkerställ att arbetsgången dokumenteras.

1 För att kunna arbeta enligt denna handbok, bör nyttjaren läsa igenom handboken och förbereda sig innan incidenthantering startar

## Anteckningar, stöd för åtgärder i din verksamhet:

# Dags att begränsa incidenten och minimera skadan.

1. Utför åtgärder som isolerar incidenten – försök att hålla incidenten till en ”plats”. Var försiktig så att verksamheten inte störs mer än vad som redan hänt. Tänk efter innan en åtgärd implementeras.

2. Vid isolering, försök identifiera vad som egentligen hänt och hur det kunde inträffa. Dokumentera.

3. Rensa ut det som inte ska finnas i system, nätverk, filer eller på konton. Var försiktig så att inte fel saker raderas. Städa smart och återställ med mjukvara från verifierade och säkra källor.

## Anteckningar, stöd för åtgärder i din verksamhet:

# Återgå till det normala, men förbättra skyddet.

1. **Påbörja återställning.** Tänk på att återställning av ett industriellt informations- och styrsystem med tillhörande stödsystem är komplext. Ta det lugnt!

2. **Följ återställningsplanen.** Det är ytterst viktigt att återställningen sker strukturerat och kontrollerat. Om det finns en återställningsplan, följ den. Om det inte finns en återställningsplan, återställ och justera endast det som måste återställas. Inför inga nya funktioner. Passa inte på att införa otestade uppdateringar, utan följ de ordinarie uppdateringsrutinerna.

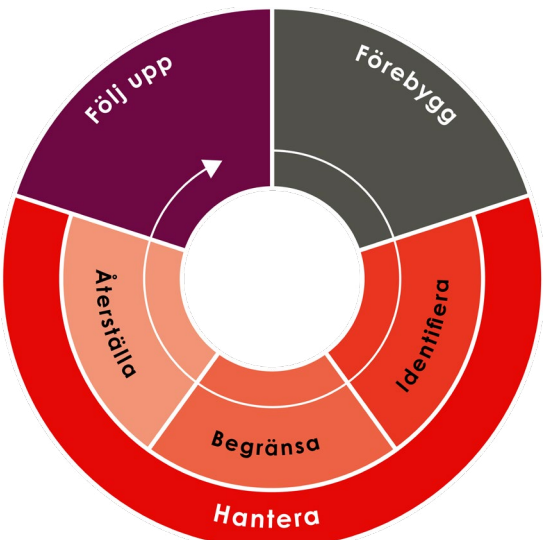
3. **Validera och övervaka.** Fungerar allt som det ska efter återställningen? Följ de ordinarie rutinerna, som vid uppdatering eller ändring av ICS-komponenter. Utöka övervakningen med exempelvis detaljerade nätverksanalyser och kontroller vid routrar och brandväggar.

4. Följ upp och förbättra incidenthanteringsplanen.

## Anteckningar, stöd för åtgärder i din verksamhet:

# Incidenthantering för cyberfysiska system

Vägledning och rekommendationer



# Förord

MSB har tagit fram denna handbok för att stödja operatörer av cyberfysiska system i sin incidenthantering.

Idén till handboken grundar sig i den ökade digitaliseringen av samhället som medför att mer information och fler it-system sammankopplas och således exponeras, vilket ökar riskerna för att de utsätts för avsiktliga incidenter. Samhällsviktiga funktioner blir alltmer beroende av att den digitala tekniken fungerar, vilket även innefattar cyberfysiska system.

Digitaliseringen medför ofta en bättre och effektivare verksamhet, men leder även till ökad sårbarhet eftersom systemen blir alltmer komplexa.

Det gör att små händelser snabbt kan utvecklas till större och mer invecklade incidenter. Därför behövs ett gediget säkerhetsarbete som tidigt kan upptäcka avvikelser och hantera incidenter.

En incident i en teknisk miljö kan vara skapad avsiktligt eller oavsiktligt. De avsiktliga incidenterna kan vara försök till eller fullbordade cyberangrepp. Dessa förekommer kontinuerligt och har idag blivit en del i den dagliga it-driften. De oavsiktliga incidenterna kan bero på allt ifrån misstag, handhavandefel och olyckor till väderförhållanden eller att tekniken fallerar.

**Frågan är inte om en verksamhet kommer utsättas för en incident, utan när.**

## Handbokens upplägg

Handboken är till för att placeras i närheten av operatörsstationer eller i utrymmen där daglig drift sker. Handboken har ifyllningsbara fält där det rekommenderas att viktig information rörande exempelvis kontaktuppgifter noteras samt övriga anteckningar som kan vara till nytta i händelse av en incident.

Handboken är uppdelad i två övergripande delar.

Den första delen, Inledning (fram till och med sidan 16) ger en introduktion till området och handboken.

Den andra delen ger vägledning och rekommendationer och är utformad enligt incidenthanteringens tre faser: förebygg, hantera och följ upp.

- Fasen förebygg beskriver det förebyggande arbetet. (sid 17 – 30)
- Fasen hantera beskriver den akuta hanteringen och erbjuder handfasta råd och rekommendationer under en pågående incident. (sid 31 – 48)
- Fasen följ upp stödjer verksamheten i uppföljningsarbetet som görs i syfte att för bättra och utveckla hanteringen av framtida incidenter. (sid 49 och framåt).

# Inledning

Handbokens rekommendationer och råd bygger på branscherfarenheter och standardiserade arbetssätt. Det finns inget färdigt recept för hur incidenthanteringsarbetet ska utformas, eftersom varje verksamhet är unik. Däremot finns ett antal vedertagna metoder som varje verksamhet bör införa för att etablera en god säkerhetskultur och ett systematiskt incidenthanteringsarbete. Verksamheten bör utveckla och implementera processer för incidenthantering. Detta för att kunna upptäcka incidenter men även kontrollera och stoppa deras orsaker samt återställa system och nätverk. Arbetet inkluderar planering, fördefinierade roller, övning, kommunikation och översyn av ledning.

## Syfte

Handboken erbjuder både aktivt stöd och djupare vägledning under hela incidenthanteringsarbetet för verksamheter som nyttjar cyberfysiska system. Handboken beskriver det förebyggande arbetet, hur den akuta fasen kan hanteras samt vägledning för att följa upp en it-incident.

## Målgrupp

Handboken riktar sig till operatörer och verksamheter som nyttjar cyberfysiska system. De olika avsnitten är riktade till olika målgrupper:

- Det inledande avsnittet och avsnittet om den *förebyggande fasen* riktar sig till ansvarig för incidenthanteringen och till de  dem som tar fram regelverk och planerar resurser.
- Avsnittet om *incidenthanteringen* riktar sig till operatörer och dem som ingår i incidenthanteringsteamet.
- Avsnittet om *uppföljning* riktar sig till alla i organisationen som deltog i incidenthanteringen.

Rekommendationerna som ges i handboken bedöms också kunna fungera som stöd utanför målgruppen.

## Avgränsningar och läsanvisningar

Incident- och kontinuitetshantering ligger mycket nära varandra. Handboken beskriver dock enbart hur en incident kan hanteras, inte hur verksamheten ska vidmakthållas.

Handboken omfattar inte tekniska detaljer eller specifika instruktioner som ska användas vid en aktiv incident, utan enbart råd och rekommenderade metoder. Handboken är inte tänkt att läsas från pärm till pärm utan att fungera som ett uppslagsverk. Längst bak finns även en ordlista.

Ha gärna handboken lättillgänglig. Verksamheten har då bättre förutsättningar att effektivt hantera en incident i både förbyggande syfte och kritiska lägen.

# Förebygg

Denna fas syftar till att skapa goda förutsättningar för att hantera en it-incident, genom att etablera rutiner, riktlinjer och en klar rollfördelning. På så sätt skapar ni en effektiv och verksamhetsanpassad struktur för att hantera incidenter. I denna fas är det även viktigt att identifiera och förebygga sårbarheter i verksamhetens system och miljö, samt analysera verksamhetens förutsättningar.

Detta avsnitt riktar sig primärt till ansvarig för incidenthanteringen dem och till dem som tar fram regelverk och planerar resurser.

## Bakgrund

Alla tekniska system har sårbarheter som kan leda till att en händelse ger negativa konsekvenser. Inom it- och ICS- eller SCADA-miljön kan dessa negativa konsekvenser resultera i stopp i produktionen, förlust eller förändring av information, eller att obehöriga tar del av skyddsvärd information.

En incident är en tillfällig störande händelse eller ett tillbud med en negativ inverkan på säkerheten i nätverk och informationssystem. En incident sker inte av sig själv, utan är ofta resultatet av en serie skeenden. Det är dessa skeenden som ska upptäckas och hanteras så att de inte leder till en incident. Att proaktivt och reaktivt ta hand om skeenden och incidenter är därför nödvändigt för att verksamheten fortlöpande ska kunna bedriva sin verksamhet.

Det är viktigt att dokumentera vad som hänt, vem som upptäckte vad och när, samt vilka åtgärder som har utförts. Dokumentationen bör innehålla vilka beslut som tas och på vilka grunder. Man dokumenterar inte för att identifiera personlig skuld eller skapar spårbarhet för att straffa misstag, utan för att förenkla incidenthanteringen. Man dokumenterar för att förenkla incidenthanteringen, samt för att möjliggöra en god överlämning till andra parter inom incidenthanteringen.

Dokumentationen ger möjlighet att utvärdera och lära av incidenten. Det minskar risken för att liknande incidenter inträffar igen, samt förbättrar verksamhetens beredskap och handlingskraft vid incidenter i framtiden. Vid brottsmisstanke är det viktigt att vara medveten om att felaktig hantering av t.ex. information i form av loggar kan innebära att viktigt underlag till en eventuell rättslig process kan förstöras.

## Bygg grunden för incidenthantering

Det förebyggande arbetet är viktigt för att skapa goda förutsättningar för incidenthanteringsarbetet. MSB rekommenderar därför att verksamheten under sin kontinuitetshantering tar fram en it-incidenthanteringsplan (fortsättningsvis kallad plan). Det är viktigt att ha en utarbetad och förberedd plan för incidenter, samt att verksamheten övar denna regelbundet.

Planen bör vara kort och begriplig för att vara användbar även i stressade situationer. Planen är tänkt att utgöra ett stöd vid en incident och används för att

- identifiera en incident,
- snabbt utvärdera situationen,
- meddela berörda personer,
- organisera åtgärder,
- dokumentera hur återställning utförs.

Planen bör även omfatta och beakta systemets eller systemens hela livscykel. Vid extrema incidenter kan det i vissa speciella fall vara mer kostnads- och tidseffektivt att utföra en större ombyggnad eller uppgradering av hela eller vissa delar av systemet, istället för att reparera eller återuppbygga ett äldre system.

Men en sådan åtgärd måste då vara väl planerat och väl testat innan ett sådant beslut kan tagas och arbete kan påbörjas.

Verksamheten ansvarar själv för att ta fram och anpassa checklistor, policyer och annat som nämns i handboken.

## Analysera verksamheten

För att kunna skapa en incidenthanteringsplan krävs detaljerad kunskap om verksamheten och processerna, som kan hämtas genom att analysera verksamheten. Hur en analys utförs och dokumenteras kan skilja sig åt, men för att ta fram en incidenthanteringsplan bör följande tre delar hos verksamheten analyseras: interna intressenter, förutsättningar och informationstillgångar.

Verksamheten bör i sin analys belysa och behandla följande frågor:

- Vad är det verksamheten gör?
- Varför gör verksamheten detta?
- Hur gör verksamheten det den gör?
- Var utför verksamheten det den gör?
- Vem utför det arbetet?
- Vilka resurser (utom information och data) behövs för att utföra arbetet?
- Vilken information behövs för att utföra arbetet?
- Hur skyddsvärd är denna information?
- Hur är den skyddsvärda informationen lagrad?
- Hur är den skyddsvärda informationen skapad, hanterad, konsumerad, ändrad och raderad?
- Hur är den skyddsvärda informationen överförd?
- Hur länge kan verksamheten vara utan den skyddsvärda informationen?
- Vem måste ha tillgång till den skyddsvärda informationen?

Analysen som ligger till grund för en incidenthanteringsplan har många likheter med den konsekvensanalys som görs i arbetet med kontinuitetshantering av verksamheten. Det är en fördel om dessa processer synkroniseras. Dels för att undvika dubbelarbete och dels för att inte missa händelser att analysera.

## Säkerställ kontinuitetshantering

Kontinuitetshantering handlar om att planera för att kunna upprätthålla verksamhet och processer och skapa en nödvändig förmåga till funktionalitet, oavsett vad som inträffar. Det kan vara när elen försvinner, vid it-störningar eller när leveranserna inte når fram.

När man tar fram verksamhetens interna regler och arbetssätt bör man planera för hur kontinuitet kan uppnås för att bibehålla information, nätverk och informationssystem vid incidenter och avvikelser. I arbetet med kontinuitetshantering skapas kännedom om verksamhetens kritiska aktiviteter, vilka resurser som de är beroende av och hur sårbara beroendena är. Det är upp till verksamheten att utifrån kontinuitetshanteringen identifiera alla beslut som behöver tas vid en incident.

**Exempel på vad som bör framgå i kontinuitetshanteringen:**

Accepterad återställningstid:

- Hur man fattar beslut om att tillämpa alternativa arbetssätt respektive beslut om att återgå till normala arbetssätt.
- Behovet av uthållighet över tid. Kontinuitetsarbetet bör utvärderas särskilt efter genomförda övningar, vid organisationsförändringar inklusive utkontraktering, vid förändrade rättsliga krav eller verksamhetskrav, samt om brister upptäcks när alternativa arbetssätt används.

Sammanfattningsvis går det utifrån verksamhetsanalysen och kontinuitetshanteringen att identifiera vilka resurser som den egna verksamheten är beroende av och vilka av dessa som är kritiska. Med hjälp av denna information kan verksamheten sedan skapa den faktiska incidenthanteringsplanen.

## Skapa incidenthanteringsgruppen[2]

Baserat på den kunskap om verksamheten som inhämtats genom verksamhetsanalysen och kontinuitetshanteringen är det lämpligt att definiera roller i incidenthanteringsgruppen (hädanefter gruppen), samt identifiera vilka personer som är lämpade att ingå. Gruppen bör ha möjlighet att samlas regelbundet för att diskutera incidenter och risker, men även kunna analysera hur dessa påverkar säkerheten i verksamhetens informations- och styrsystem.

En viktig sak att beakta i verksamhetsanalysen är externa beroenden och beroendekedjor, exempelvis om verksamheten är beroende av extern specialistkompetens bör denna säkras i förhand, exempelvis genom avtal eller överenskommelser.

Gruppen bör bestå av representanter från ledningen, samt representanter från både processkontroll- och it-sidan:

- CSO, CISO eller CIO, som representerar ledningen
- Tekniska chefer, representanter för säkerhet, nätverk, it, ICS
- HR, för att hantera personella resurser (övertid, löner m.m.)
- PR eller Kommunikation, för att hantera extern kommunikation
- Jurist (vid behov)
- Affärsområdesexperter (vid behov)

Hur gruppen är sammansatt är upp till verksamheten att själv bestämma. Ofta finns två alternativ:

- Fastställd grupp som alltid har denna sammansättning.
- En mindre kärngrupp, där sedan experter kan inkallas.

2. För vidare läsning, se avsnittet *Läs mer* längst bak i handboken.

## Definiera och fastställ roller och befogenheter

Observera att roller utan befogenheter är direkt motverkande i en incidenthanterande verksamhet. För att minimera risken att det uppstår missförstånd i stressade situationer, som leder till att dyrbar tid går förlorad, är det av yttersta vikt att beslutsvägar, roller och befogenheter är definierade. Följande frågor bör besvaras:

- Vem eller vilka har rätt att definiera något som en incident?
- Vem eller vilka har rätt att sammankalla incidenthanteringsgruppen?
- Vem eller vilka har rätt att stoppa delar av verksamheten?
- Vem eller vilka har rätt att besluta att växla över till alternativ drift?

## Definiera när gruppen ska sammankallas

Verksamheten bör utreda och definiera i vilka situationer gruppen ska sammankallas. Detta kan göras genom att fastställa tröskelvärden och kategorisera exempelvis indikation på typ av incident, konsekvens och art. Exempelvis kan en mindre del av gruppen sammankallas vid mindre omfattande incidenter. Det bör även klarläggas inom vilka tidsgränser gruppen ska kunna sammankallas eller kontaktas, och vilka kommunikationsvägar som ska nyttjas.

## Tidsaspekten och den utopiska 1-10-60 "regeln"

Avgörande för incidenthantering är tidsaspekten. Den påverkar i hög grad hur incidenten fortskrider och dess konsekvenser. Verksamheten har begränsat med tid att upptäcka och åtgärda en incident innan den sprids.

En riktlinje att förhålla sig till för tidsfördelning av arbetsinsatser är 1-10-60-minuters ”regeln”.

1-10-60-minuters ”regeln” är en utopi, där verksamheten bör sträva efter följande tre tidsaspekter:

- **1 minut** – tiden verksamheten har på sig för att upptäcka en incident.
- **10 minuter** – tiden verksamheten har på sig för att utreda samt förstå incidentens allvarlighetsgrad och mål. Här bör verksamheten även lägga fram nödvändiga motåtgärder.
- **60 minuter** – tiden verksamheten har på sig för att hantera incidenten och implementera åtgärder.

Observera att 1-10-60 ”regeln” är ofta inte realistisk förutom i specifika situationer och i verksamheter som arbetar med kontinuerlig incidenthantering.

Trots att det kan vara utmanande och tidsaspekten är kritisk, gäller det att vara systematisk, strukturerad, noggrann och gå på fakta. Ta ett steg tillbaka och analysera läget. Tänk efter innan en åtgärd implementeras. Ta det lugnt!

## Kontaktytor och kommunikation

I händelse av en incident är kommunikation vital, för att spara tid. I och med detta måste följande fastställas:

- Vilka kommunikationsvägar som ska nyttjas.
- Hur gruppen ska kommunicera säkert (är det säkert att använda verksamhetens system, såsom e-post?).
- Var ska gruppen mötas, finns det en ledningsplats?
- Vad ska kommuniceras muntligt och vad ska kommuniceras skriftligt?

Utöver detta måste det bestämmas vem som ska kommunicera med externa parter, såsom

- extern teknisk hjälp,
- tillsynsmyndigheter,
- brottsbekämpning,
- media,
- försäkringsbolag,
- eventuell extern advokat.

Fastställ även vem som ska rapportera till företagsledare och styrelse. Oftast brukar det vara CSO, CISO eller CIO som är en del av incidenthanteringsgruppen.

## Avgör om det behövs extern teknisk hjälp

När man genomför analys och kontinuitetshantering är det viktigt att avgöra om verksamhetens egna resurser är tillräckliga för att hantera en incident, eller om det behövs extern hjälp. Extern hjälp bör vara avtalad innan en incident inträffar.

Det är verksamhetens behov som avgör ifall extern hjälp ska avtalas, eftersom det kan vara en kostnad att ha möjlighet att avropa resurserna. Det är också viktigt att vara medveten om att även andra organisationer kan göra motsvarande avtal med resursen, och att det vid en större incident kan bli en konkurrenssituation om vilken organisation som verkligen får en leverans. Frågor som dessa bör hanteras i avtalet.

## Säkerställ rapportering

I samband med att en incident upptäcks, kan rapportering behöva göras till berörda parter. Rapporteringen ska utföras i enlighet med de lagrum och föreskrifter som reglerar verksamheten. Verksamheten bör redan i det förberedande arbetet ha arbetat fram rutiner, inhämtat mallar för vad en incidentrapport ska innehålla, samt fastställt kontaktuppgifter till relevanta instanser.

**Följande frågor bör besvaras:**

- Vilka rapporteringskrav har verksamheten?
- Vem eller vilka ska rapporteras till?
- Vad ska rapporteras?
- I vilket format bör rapporten vara?
- Vad är målet med rapporteringen?

Verksamheten ansvarar själv för att undersöka och fastställa var, när och hur den ska rapportera it-incidenter.

## NIS-direktivet

Under 2018 infördes NIS-direktivet i Sverige. Det omfattar leverantörer av samhällsviktiga tjänster och vissa digitala tjänster. Direktivet ställer krav på att tjänsterna ska bedrivas genom ett systematiskt och riskbaserat informationssäkerhetsarbete, med stöd i specifika standarder. Det ställer även krav på dokumentation, informationssäkerhet och incidentrapportering i nätverk och informationssystem. Samhällsviktiga tjänster och verksamheter finns i både den privata och offentliga sektorn och är uppdelade i sju sektorer:

- Energi
- Transport
- Bankverksamhet
- Finansmarknadsinfrastruktur
- Hälso- och sjukvård
- Leverans och distribution av dricksvatten
- Digital infrastruktur

Den som identifierat sig som en leverantör av samhällsviktiga tjänster är anmälningspliktig. Stöd finns i MBS:s föreskrifter för anmälan och identifiering av leverantörer av samhällsviktiga tjänster. MSB och tillsynsmyndigheterna kopplat till NIS har föreskriftsrätt. Föreskrifterna finns på MSB:s webbplats, www.msb.se/nis.

**Lag och förordning för NIS**

Lag 2018:1174 om informationssäkerhet för samhällsviktiga och digitala tjänster.

Förordning 208:1175 om informationssäkerhet för samhällsviktiga och digitala tjänster.

## Testa, öva och utvärdera

Många verksamheter har tagit fram dokumentation men aldrig testat den, eller så har verksamheten inte övat enligt planerna. Det kan även vara så att medlemmar i incidenthanteringsgruppen träffas för första gången när en incident väl inträffar. Men förtroende och personkemi är en viktig parameter för att säkerställa en lyckad incidenthantering och kunna agera enligt plan i en stressande situation. Därför är det viktigt att testa, öva och utvärdera innan en incident inträffar. Detta bör göras när verksamheten tagit fram verksamhetsanpassade policyer, kontinuitetsplaner, rutiner m.m. Det kan göras på olika sätt, t.ex. genom strukturerade seminarieövningar. Det finns även simuleringsövningar där incidentgruppen samlas och spelar igenom ett tänkt scenario för att se om det som står i planen och övrig dokumentation är tillräckligt.

När planen är testad måste en utvärdering göras för att identifiera om planen behöver revideras, eller om andra parametrar (t.ex. incidenthanteringsgruppens sammansättning) behöver justeras. Vid utvärderingen kan det visa sig att enkla utmaningar (t.ex. att VoIP eller mobiltelefoni är otillgänglig eller begränsad) kan orsaka större utmaningar, eftersom flera problem behöver lösas samtidigt som incidenten. Parallella problem i kombination med begränsade resurser kan leda till negativa konsekvenser vid en riktig incident.

## Simuleringsövningar kan bidra till att:

- Pröva och utveckla den plan som testas, samt identifiera dess brister och avvikelser.
- Stärka incidenthanteringsgruppens interna kommunikation och förtroende.
- Låta deltagarna bekanta sig med sin roll och sina befogenheter, samt vilka kriterier som är underlag för vilka beslut.
- Öka förmågan att fatta snabba beslut och delge lägesinformation.
- Upprätthålla medvetenheten om den komplexitet som är karaktäristisk för krissituationer.
- Visa på områden där ytterligare utbildning eller träning behövs.
- Belysa svagheter och styrkor i resurser och teknik.
- Öka det allmänna medvetandet om styrkor, möjligheter och brister, och vid behov utveckla deltagarnas skicklighet och tillit till sin egen kompetens.

Det är viktigt att öka verksamhetens medvetenhet om att en it-incident är dynamisk. Oavsett hur väl förberedd och planerad incidenthanteringen är, är det svårt att identifiera och korrekt anpassa samtliga parametrar.

# Hantera

När en it-incident inträffar är det viktigt att handla målinriktat och effektivt för att förhindra ännu större negativa konsekvenser. Det finns en mängd åtgärder att vidta för att hantera en incident. MSB rekommenderar att verksamheter tar ett systematiskt grepp om it-säkerhetsarbetet för att säkerställa att hanteringen av incidenter blir effektiv och framgångsrik. Det är ytterst viktigt att verksamheten redan i den förberedande fasen definierat vad en potentiell risk innebär och när incidenthanteringsprocessen ska börja. Verksamheten måste själv identifiera och specificera hur uppgifter och processer korrelerar, hur informationsflöden dokumenteras och hur åtgärdsarbetet koordineras.

MSB väljer här att dela upp incidenthanteringen i tre delmoment: **identifiera**, **begränsa** samt **återställa**. Städa och återställa är nära relaterade.

Detta avsnitt riktar sig primärt till operatörer och dem som ingår i incidenthanteringsteamet.

## Delmoment 1: Identifiera incidenten

Processen startar med att identifiera om det är en faktisk incident. Det är också viktigt att avgöra huruvida en incident inträffat eller eventuellt pågår just nu. I båda fallen behöver man ta reda på incidentens typ, utbredning samt konsekvenser för verksamheten.

**Verksamheter möter initialt ofta fyra utmaningar i detta arbete:**

- Upptäcka en incident (t.ex. övervaka och samla in information kring avvikelser eller fastställda tröskelvärden som när de passeras ska kunna ge en indikation av en händelse).
- Ha en förmåga att kunna göra bedömningar utifrån den i många fall begränsade information som finns tillgänglig.
- Avgöra typ av händelse, t.ex. om den har sin grund i DDoS, skadlig kod, sessionskapning eller handhavandefel.
- Baserat på bedömningen kunna ta beslut om huruvida det är en incident som ska hanteras inom incidenthanteringsplanen, eller om det är en avvikelse som kan hanteras inom linjeverksamheten.

## Detektera en möjlig incident

Den viktigaste resursen att upptäcka en möjlig incident är människan. Det är därför viktigt att verksamheten

- tar vara på sina medarbetares erfarenheter och kompetens, samt skapar en tydlig rollfördelning,
- konstruerar och förmedlar viktig kontaktinformation.

Detekteringsprocessen ämnar identifiera avvikande nätverksaktivitet eller misstänkta händelser som kan äventyra verksamhetens informationssäkerhet. Det finns en mängd olika möjliga verktyg för detektering, med differentierad grad av precision, t.ex.

- alarm genererade av tekniska övervakningssystem (t.ex. Data Loss Prevention (DLP), dataintrångsdetekteringssystem (IDS), antivirusprogram samt systemstöd för logganalys)
- rapporterad misstänkt händelse (t.ex. från användare till it-kundtjänst eller direkt till säkerhetsavdelning via operatören)
- avvikelser upptäckta vid revision, utredning eller utvärdering.

Det kan dagligen inkomma tusentals möjliga tecken på negativ händelse till en verksamhet. Dessa kan kategoriseras utefter tecken på att en incident kan inträffa i framtiden, **avvikelser**, eller tecken på att en negativ händelse kan pågå, **indikatorer**.

| Exempel på möjliga incidenter | Källor till tröskelvärden |
|---|---|
| **Avvikelser** kan inkludera:<br>• Anomalier i loggar samt upptäckt av skadlig kod.<br>• Meddelande om försök till intrång på känsliga servrar.<br>• Hot om intrång och planerad attack mot verksamheten. | • Säkerhetsprogram (t.ex. IDS, IPS, DLP, SIEM, antivirus- och antispamverktyg, monitoreringsprogram).<br>• Säkerhetsloggar från operativsystem, applikationer och tjänster, nätverksenheter och nätverkstrafikfilter.<br>• Publikt tillgänglig information[3] (t.ex. nyheter om nya tekniker för att utnyttja sårbarheter, nätverksinformation, tredjepartsinformation).<br>• Människor inom organisationen. |
| **Indikatorer** kan inkludera:<br>• Antivirusprogram som sänder ut alarm vid upptäckt av skadlig kod som infekterar enheter.<br>• Systemadministratör som påträffar anomalier i loggar.<br>• Applikationsloggar som påvisar flera misslyckade inloggningsförsök från främmande externt system.<br>• Mejladministratör som påträffar att mängder med mejl med misstänkt innehåll studsat. | |

3. För vidare information se www.msb.se/ics eller www.cert.se.

Att detektera en incident genom övervakning är en stor utmaning. Alltför ofta implementerar verksamheter ett IDS för övervakning men lämnar systemet därefter åt sitt eget öde, utan mänsklig kontroll. För fungerande och god detektering rekommenderar MSB därför att övervakning sker

- vid alla möjliga exponerade kommunikationspunkter,
- systematiskt – för att inte riskera att förbise en avvikelse eller reagera på ett falskt larm,
- aggregerande, vilket innebär att analysera helheten för att skapa en överblick.

MSB rekommenderar att verksamheter tar ett systematiskt grepp om incidenthanteringen och att detektion och analys utförs i hela verksamheten. Vidare rekommenderar vi verksamheter att rapportera incidenter som allvarligt kan påverka säkerheten till relevanta kontakter:

- dokumentera all viktig information och alla steg i incidenthanteringsarbetet (typ av incident, meddelande på skärm, detaljer kring anomalier),
- vara återhållsamma vid försök att åtgärda en upptäckt incident, överväga konsekvenser och om möjligt analysera incidenten djupare innan åtgärder vidtas,
- vidta relevanta steg utefter sin incidenthanteringsprocess.

## Definiera en incident

När en incident detekterats övergår arbetet i att definiera dess konsekvenser, alternativt dess mål. Detta för att verksamheten ska kunna utforma korrekta och effektiva åtgärder, avgöra potentiell resursanvändning och korrekt prioritet och kunna lösa incidenten inom rimlig tid – men även för att verksamheten ska kunna utreda och lära av situationen. Följande frågor bör, om möjligt, besvaras i denna fas:

- Varför har incidenten eller attacken inträffat?
- Hur kunde incidenten inträffa (t.ex. vilka sårbarheter utnyttjades, vilka metoder använde en eventuell angripare)?
- När ägde incidenten rum?
- Vilken typ av information har blivit drabbad eller hamnat i otillbörliga händer, blivit stulen, raderad eller förändrad?
- Identifiera vilka system, nätverk eller databaser som blivit drabbade:
  - Är identifierade system intakta?
  - Har nätverk kopplats bort?
  - Förvaltas det påverkade systemet av egen eller extern organisation?
  - Kan eller får system stängas ner?
- Avgör skadan och den negativa affärspåverkan.
- Gör en detaljerad analys av incidenten:
  - Vilka observationer är gjorda?
  - Hur upptäcktes problemet?
  - Vilken typ av loggar finns att tillgå?
  - Vilka typer av system loggar?

## Sortera och prioritera

Efter att en incident har detekterats och definierats, kan åtgärderna sorteras och prioriteras. Det är i denna fas verksamheten avgör om utredning och begränsning av händelsen ska påbörjas, eller om händelsen är att kategorisera som ett falskt alarm och kan hanteras inom den ordinarie linjeverksamheten.

Det krävs en initial analys av en incident för att avgöra dess utbredning, påverkan och konsekvens på verksamheten. Följande metoder kan användas:

- Intelligensbaserad metod, baserad på den insamlade informationen från myndigheter, egna övervakningsmekanismer, information från öppna källor eller internt inhämtad information.
- Evidensbaserad metod, baserad på information insamlad via verksamhetens egen infrastruktur eller applikationer (typiskt loggar).

Om det tar för lång tid från att en incident upptäcks tills den varnas för och hanteras, kan omfattning, resursanvändning och återställningstid bli betydligt större än om incidenten hade hanterats tidigt och kategoriserats korrekt. Det är även skillnad på om incidenten precis uppstått och spridningen eskalerar, eller om den har funnits i systemet en längre tid och är i vilande läge. Val av åtgärder och hur snabbt verksamheten bör agera, bör bedömas utefter incidentens typ, verkan och konsekvens.

För att personal och verksamhet inte ska riskera att drabbas av utmattning, är det viktigt att processen för analysen utformas effektivt och tillförlitligt. Berörd personal rekommenderas att:

- utvärdera viktiga alarm eller misstänkta händelser i loggar eller via tekniska övervakningssystem (t.ex. IDS, IPS, DLP eller SIEM),
- koppla denna information till nätverksdata (inklusive data från molntjänster),
- jämföra dessa gentemot riskinformation och hotbild.

Dokumentera och utred även följande:

- datum och tid,
- internetprotokoll (IP) och adresser (interna eller externa),
- portar (källa eller destination), domäner och filer (t.ex. .exe, .dll),
- system (hårdvaruförsäljare, operativsystem, applikationer, mål och syfte, plats).

## Tips och rekommendationer

Det kan vara bra att initialt agera med full kraft för att effektivisera processen. Ändå är det inte alltid att rekommendera, eftersom ett mer återhållsamt tillvägagångssätt kan vara avgörande för att korrekt definiera en incident. Här är några tips för ett lyckat förfarande:

- Kontrollera information som rör händelsen. Exempelvis, om en ändpunkt visar tecken på virus, kontrollera om viruset är aktivt på enheten innan du påkallar ytterligare åtgärder.
- Förstå kontexten i vilken informationen befinner sig. Bara för att IP-adressen flaggades som del av ett botnät föregående vecka, måste det inte det vara så denna vecka.
- Ensa insatserna med operationella prioriteringar och definiera incidenten ändamålsenligt. Säkerställ att varje rapporterad incident ges rätt åtgärd och prioritering.
- Sök efter och analysera eventuella likheter, som IP-adresser och domäner över flertalet databaser, för bästa möjliga dataskärpa.

Medverka gärna i något av MSB:s forum för informationsdelning[4] eller liknande nätverk, och registrera er verksamhet för CERT:ens informationsutskick och lägesuppdateringar[5]. När händelser är verifierade övergår arbetet i att begränsa incidentens eventuella åverkningar, för att i ett senare skede följa upp det inträffade och utveckla verksamhetens robusthet, s.k. ”raising the bar”. Vi rekommenderar att alla detekterade och definierade incidenter utreds och följs upp med målet att utveckla verksamheten inför framtida incidenter.

4. Bl.a. FIDI-Scada
5. www.cert.se

## Delmoment 2: Begränsa och städa

Vid upptäckt av skadlig kod bör verksamheten agera snabbt för att minimera skadans effekt och spridning i system, nätverk och enheter, såväl i verksamheten som utanför. Det är komplext att upprätthålla verksamheten i ett normalt funktionsläge samtidigt som system begränsas i syfte att minimera risker. Beroende på typ av incident är olika begränsningsåtgärder lämpliga. För att förenkla beslutsprocessen bör kriterierna vara tydliga för val av åtgärder, exempelvis:

- Potentiell skada och stöld, förändring eller borttagande av data och/eller information.
- Behov av bevis för bevarande.
- Kritisk nivå på det berörda systemet.
- Systemets krav på tillgänglighet (t.ex. nätverkskoppling och service andra parter berörs av).
- Effektivitet vid val av strategi (t.ex. delvis eller full begränsning av system).
- Omfattningen av tid och resurser som krävs för att utnyttja en strategi.
- Lösningens varaktighet (t.ex. nödlösning eller annan tillfällig lösning).
- Hur felsäker den valda strategin är.
- Vad är verksamhetens mål med arbetet mot incidenten?
  - Polisanmäla och åtala angripare?
  - Avbryta angreppet så snabbt som möjligt?
  - Återställa systemet så snabbt som möjligt?
  - Låta systemet vara intakt och ta upp ett nytt system parallellt?

## Isolera

Beroende på typ av incident och dess konsekvenser på verksamheten bör olika åtgärder vidtas, vilka kan fastställas redan i kontinuitetshanteringen. Viktigt att bestämma är huruvida det infekterade systemet ska bortkopplas från verksamheten direkt, eller vara i fortsatt funktionsläge i syfte att samla in information om incidenten?

Isolation av påverkade system kan minimera skadans omfattning och påskynda återgången till normal verksamhet när incidenten väl är över. Om incidenten hotar integriteten i nätverk, eller andra kopplade system, bör det bortkopplas snarast möjligt. När det gäller kritisk verksamhet utan tillgång till backupsystem, kan bortkopplandet av system från nätverk leda till förödande konsekvenser eftersom verksamheten inte hålls kontinuerligt och normalt fungerande.

**Exempel på sätt att begränsa spridning av skada:**

- Blockera (och logga) auktoriserad tillgång till system.
- Begränsa nätverkstrafiken.
- Byt administratorslösenord där intrång misstänks.
- Tillämpa tvåfaktorauktorisering.
- Brandväggsfiltrera eller installera en router med ACL.
- Omdirigera webbsidors hemadresser.
- Isolera eller stäng av system.
- Koppla bort ström från centrala servrar.
- Isolera vissa tjänster från övrig it-infrastruktur.

## Utreda

Att bibehålla system i fortsatt funktionsläge möjliggör en djupgående analys av incidentens grundorsak och verkan, samt ger förutsättning för långsiktig sanering. När system hålls kvar i drift kan lämpliga förändringsåtgärder för påverkade processer göras, t.ex. byta inloggningsuppgifter och isolera påverkade processer från varandra samt övervaka system och loggar. För att utreda incidenten och identifiera uppkomsten, krävs att information, material och bevisföring dokumenteras tydligt inför en it-forensisk utredning.

## Städa

Att städa system involverar att ta bort skadlig kod, konton, material och olämplig tillgång till system och information. Fasen omfattar även att åtgärda de sårbarheter som legat till grund för incidenten. Om möjligt bör en total återställning göras av operativsystem och applikationer. Städningen bör utföras med precision och snabbhet för att skador inte ska hinna återetableras innan systemet är städat och säkrat.

**De generella stegen i städningen är följande:**

- Identifiera och mildra alla utnyttjade sårbarheter och värddatorer inom verksamheten.
- Ta bort skadlig kod, olämpligt material och andra artefakter som incidenten orsakat.
- Undersök om städningen av systemen besvaras av en eventuell angripare genom förändring av attackmetod eller attackmönster.
- Om ytterligare värdar upptäcks vara infekterade, upprepa identifierings- och begränsningsfaserna för att identifiera alla påverkade system och fortsätt med begränsning och städning.
- Ominstallera operativsystem och applikationer, och tillämpa kända uppdateringar av programvara. Beroende på typ av incident och hur pass kritiskt systemet är, är det ibland enbart rekommenderat att rensa ut och uppdatera systemen.
- Förbered och utveckla ytterligare åtgärder ifall en eventuell angripare byter typ av angrepp.
- Utför en sårbarhetsanalys kontinuerligt.
- Fortsätt städa tills avvikelser inte längre observeras i nätverkstrafik och system.

## Delmoment 3: Återställa

I denna fas återställer verksamheten det utsatta systemet för att återgå till normalt funktionsläge. Under återställningsfasen bör, om möjligt, identifierade sårbarheter åtgärdas med syfte att förebygga liknande framtida incidenter. Det är viktigt att eventuell ny funktionalitet testats ordentligt innan den implementeras, för att undvika att nya sårbarheter tas i drift. Det kan bli mycket tidskrävande att införa ny funktionalitet. Gör därför en avvägning av om det är möjligt eller värt att fördröja återställningen för att införa den nya funktionaliteten.

**Återställning kan göras på flera olika sätt:**

- Byt ut infekterade filer mot ”rena versioner”, det vill säga filer från verifierade och säkra källor.
- Bygg systemet från grunden med ny hårdvara eller mjukvara.

## Att tänka på vid återställning

Incidenthantering inom cyberfysiska system skiljer sig från incidenthantering i kontorssystem på så sätt att vissa processer inte kan stängas ner. Avbrott i vitala processer inom cyberfysiska system kan medföra allvarliga konsekvenser beroende på verksamhet. Vad som är gemensamt för de flesta verksamheter är att dessa avbrott tenderar att bli mycket kostsamma.

Problem kan uppstå när en återläsning från backup inte fungerar. Det är därför viktigt att utföra regelbundna kontroller av backupsystem och utrustning, och utgå från verksamhetens krav på återställning och tillgänglighet i utformning och design av backupsystemen.

**För att minska risken för problem i återställning av nätverk bör följande ses över:**

- förändringar hos internetleverantören,
- förändrade brandväggsregler,
- förändringar i routerkonfigurationer,
- förändringar i switchar.

**Tänk på att:**

- Trots att man rensar ut alla identifierat infekterade filer finns risk att oidentifierat infekterade filer finns kvar.
- Det är viktigt att regelbundet kontrollera att backuper är fria från skadlig kod.
- Att bygga upp systemet från grunden är dyrt, men garanterar att systemet helt blir av med den skadliga koden.

## Följ återställningsplanen

För att kunna genomföra återställning så snabbt och säkert som möjligt är det bra att ha en återställningsplan. Planen utgör ett hjälpmedel i arbetet att återställa systemet i enlighet med verksamhetens krav på återställning och tillgänglighet.

Sätt en återställningsplan i verket under eller efter incidenten. Åtgärderna kan variera beroende på typ av incident, men kan inkludera att

- återuppbygga system,
- återställa, återskapa eller rätta felaktig information och maskin- och programvara,
- byta ut infekterade filer mot rena versioner av filerna,
- ta bort tillfälliga begränsningar som införts under begränsningsfasen,
- återställa lösenord på utsatta konton,
- installera uppdatering, byta lösenord och säkra upp nätverket genom diverse åtgärder (exempelvis ACL),
- genomföra systemomfattande testning, säkerhetskontroller och integritetskontroller,
- ange hur man verifierar att saneringen av angripna system har lyckats och att de är fullt återställda,
- återaktivera överflödiga resurser som förlorades eller skadades under incidenten,
- återställa konfigurationsinställningar med eventuella anpassningar,
- återupprätta tjänster som stoppades under händelseförloppet.

## Validera och monitorera

Innan systemet åter tas i drift bör det testas för att säkerställa att alla funktioner fungerar som de ska. Det finns till exempel verktyg som kan användas för att identifiera eventuellt kvarstående sårbarheter. Nätverket bör monitoreras kontinuerligt för att kunna identifiera ytterligare attacker eller försök till attacker. Extra resurser kan behöva läggas på monitorering under perioden efter en återställning.

# Följ upp

Det huvudsakliga syftet med uppföljning är att verksamheten ska identifiera lärdomar och erfarenheter från incidenten. Detta för att införa eller förbättra åtgärder (både tekniska och administrativa) i syfte att förebygga framtida incidenter eller möjliggöra en mer effektiv incidenthantering. Vid återgång till normal drift finns det möjlighet att bedöma incidentens omfattning, samt vilka konsekvenser den fått för verksamheten. Under uppföljning bör verksamheten göra följande:

- Utvärdera och dokumentera vilka grundorsaker som möjliggjort att incidenten kunnat inträffa, samt vilka brister i verksamheten som medfört detta.
- Sträva efter att fastställa vilken typ av skadlig programvara som påverkat verksamheten, hotaktör, angreppsvektor, verktyg och hur händelseförloppet utvecklats.
- Diskutera och utvärdera avslutad incidenthantering. Kartlägga hur effektivt incidenthanteringens beståndsdelar, såsom processer, metoder, riskbedömningar, säkerhetsåtgärder, rapporteringsformat och organisationsstrukturer har fungerat.
- Uppdatera och åtgärda brister och förbättringspunkter utifrån identifierade lärdomar.
- Se till att kommunikationen mellan berörda parter är tydlig, koncis och fokuserad på problemlösning och kontrollförbättring. Lägg inte skuld på en enskild person.
- Kommunicera och dela resultaten av erfarenheterna med relevanta intressenter, tillämpa lämpliga kompetenshöjande åtgärder samt medvetandegör hos anställda.

**Följande frågor kan vara till hjälp under en uppföljning:**

- Hur väl hanterade och följde personal samt ledning dokumenterade rutiner?
- Var rutinerna lämpligt utformade?
- Vilken information behövdes i ett tidigt skede?
- Utfördes några åtgärder som motverkade målet med incidenthanteringen?
- Hade oförutsedda händelser kunnat motverkas?
- Hur kan personal och ledning förbättra sitt agerande inför kommande incidenter?
- Vilka åtgärder kan motverka liknande incidenter i framtiden?
- Vilka avvikelser eller indikationer kan uppmärksammas i framtiden för att upptäcka liknande incidenter?
- Vilka är lärdomarna från incidenten?
- Behöver rutiner eller policyer ses över och förändras?
- Medför incidenten att större systemförändringar bör genomföras?
- Medför incidenten att förändringar bör göras i skalskyddet?
- Hur sköttes kontakter med media?

## Implementera åtgärder

Efter utvärdering av incidenten är det viktigt att översätta resultatet i konkreta åtgärder. Det kan t.ex. innebära förändringar i incidenthanteringsrutinerna, nya eller uppdaterade förebyggande övningar, uppdatering av material, införande av tekniska kontroller, eller förändrade krav på säkerhetsåtgärder, riktlinjer samt hot- och sårbarhetsinformation.

Åtgärder av teknisk natur ska implementeras enligt plan och vi rekommenderar att åtgärderna testas innan de sätts i bruk i ett kritiskt läge. Nya och otestade tekniska lösningar bör införas först efter att incidenten är omhändertagen, inte under en tid av stress och kris i en verksamhet.

En del tekniska åtgärder som införs för att hantera en incident kan vara temporära. Det är vitalt att identifiera och dokumentera dessa som ”tillfälliga lösningar”. När incidenten är omhändertagen ska dessa reservrutiner antingen bytas ut eller kompletteras och fullständigt dokumenteras enligt verksamhetens regelverk, om de sedan ska övergå till att användas även i normal drift.

Åtgärder som ska utföras efter en incident kan även vara av administrativ eller personell natur, vilket kan glömmas bort eller nedprioriteras i det tekniska perspektivet. Det är vitalt att fånga upp och införa sådana åtgärder som ett led i att höja beredskapsnivån inom verksamheten.

**Exempel på ”förbisedda” åtgärder i kritiska lägen:**

- Införa temporära platser för vila eller sömn för att säkerställa återhämtning.
- Säkerställa måltider och fika utanför kontorstid.
- Säkerställa kommunikation och stöd till familjer och anhöriga om personalen måste arbeta utanför kontorstid.
- Hantera ekonomisk ersättning för personalen (eller informera om detta).

Många av dessa åtgärder brukar lösa sig under en incident, men tar värdefull tid från den ordinarie incidenthanteringen. Tid är den mest kritiska parametern vid en stor incident.

## Läs mer

MSB har tagit fram vägledande material som riktar sig till verksamheter i syfte att utveckla och öva deras säkerhetsarbete. Målet är bland annat att verksamheterna ska öka medvetenheten om informationssäkerhetens betydelse, tillämpa systematiskt informationssäkerhetsarbete och utföra rekommenderade säkerhetsåtgärder.

- Övningsvägledning, www.msb.se/sv/utbildning--ovning/ovning/
- Säkerhet i ICS, www.msb.se/ics
- Elektromagnetiska hot, www.msb.se/elektromagnetiskahot
- Fysisk informationssäkerhet, www.msb.se/sv/publikationer/vagledning-for-fysisk-informationssakerhet-i-IT-utrymmen/
- Kontinuitetshantering, www.msb.se/kontinuitetshantering
- CERT-SE https://www.cert.se/

**Mer information finns på MSB:s webbplats, www.msb.se.**

### Skyddspaket för ICS och SCADA

Skyddspaketet är en samling mjukvaruverktyg som underlättar för operatörer av ICS och SCADA att förbättra sin informations- och cybersäkerhet. Det är fem verktyg som ger ett grundskydd och levereras i form av delverktyg baserade på öppen källkod. Verktygen innefattar logginsamlingsserver, nätverksinspelningsserver, larmserver, IDS-server samt brandvägg för ICS- och SCADA-miljö.

**Mer information finns på www.informationssäkerhet.se.**

# Externa vägledningar och rekommendationer

För att skapa en incidenthanteringsgrupp rekommenderas följande guider och material:

## FIRST – Forum of Incident Response and Security Teams:

- Allmänna tips och råd: https://www.first.org/resources/guides/
- Etablera en CERT: https://www.first.org/resources/guides/#CERT-in-a-box
- Eller https://www.first.org/resources/guides/Establishing-CSIRT-v1.2.pdf
- Faktablad på området: https://www.first.org/resources/guides/Factsheet_Building_a_SOC_start_small.pdf

## RFC 2350:

- Etablera en CSIRT: https://tools.ietf.org/html/rfc2350

## ENISA – European Union Agency for Cybersecurity

- Handböcker, vägledningar samt utbildningar: https://www.enisa.europa.eu

# Ordlista

| | |
|---|---|
| **ACL (Access Control List)** | En lista med regler för vad som tillåts eller inte, används bl.a. i filsystem och routrar. |
| **Botnät** | En mängd enheter kopplade till internet som olovligen kan användas av en och samma aktör. |
| **CIO** | Eng. Chief Information Officer. |
| **CISO** | Eng. Chief Information Security Officer. |
| **CSO** | Eng. Chief Security Officer. |
| **DDoS (Distributed Denial of Service)** | Ett stort antal datorer som samtidigt används för att överbelasta en mottagare genom att sända stora mängder data. |
| **DLP (Data Loss Prevention)** | Ett system eller en samling verktyg som genom övervakning av nätverket används för att undvika eller minimera dataförlust. |
| **DNS (Domain Name System)** | Domännamnsystemet sammankopplar och översätter domännamn till IP-adresser för datorer, tjänster eller resurser uppkopplade till internet. |
| **Domän** | Del av internet, namngiven genom DNS-systemet. |
| **Handhavandefel** | Felaktig hantering som avviker från den förväntade hanteringen. |
| **HR (Human Resources)** | Verksamhetens personalavdelning – benämns ofta med den engelska förkortningen HR. |

| | |
|---|---|
| **ICS (Industrial Control Systems)** | En vanligt förekommande förkortning som ibland används synonymt med industriella informations- och styrsystem. |
| **IDS (Intrusion Detection System)** | Ett system som används för att upptäcka nätverksintrång. |
| **Incident** | Oönskad händelse som kan leda till negativ påverkan på verksamheten. |
| **ISP (Internet Service Provider)** | Nätverksleverantör. |
| **IT-forensik** | Kriminalteknisk undersökning av brottsspår i it-system. |
| **NIS-direktivet** | NIS-direktivet är ett EU-direktiv som i korthet innebär krav på informationssäkerhet och incidentrapportering för leverantörer av samhällsviktiga och vissa digitala tjänster. NIS står för nätverks- och informationssystem. |
| **PR (Public Relations)** | Arbetet med att främja organisationens anseende. |
| **Raising the bar** | Ett idiomatiskt utryck som i denna handbok avser beskriva en ökning av motståndskraften mot cyberhot och cyberattacker genom att förbättra standarden på åtgärder. |
| **Risk- och sårbarhetsanalys** | Används som ett verktyg för att identifiera risker och sårbarheter med syftet att reducera risker, minska sårbarheter och förbättra förmågan att förebygga, motstå och hantera kriser och extraordinära händelser. |
| **Robusthet** | Förmåga hos ett system att tolerera störningar och fel. |
| **SCADA (Supervisory Control and Data Acquisition)** | Ett övergripande, ofta geografiskt distribuerat, industriellt styrsystem för övervakning och styrning av processer för industriellt bruk. |

| | |
|---|---|
| **Sessionskapning** | (Eng. Session Hijacking) Olovligt övertagande av en valid och pågående datorsession. |
| **SIEM (Security Information and Event Management)** | Ett SIEM-system samlar in data från ett flertal system och analyserar data i syfte att hitta tecken på angrepp. |
| **Skadlig kod** | Oönskad kod som leder till negativ påverkan på verksamheten. |
| **Stödsystem** | I denna handbok avses it-system som har till funktion att stödja ICS- och SCADA-system med tekniska funktioner, exempelvis centraliserad autentisering och logg. |
| **Sårbarhet** | Avsaknad eller brist i en struktur som skulle kunna förhindra eller bidra till att förhindra att en incident inträffar. Alternativt förhindra eller bidra till att mildra konsekvensen av en incident. |
| **Tillsynsmyndighet** | Myndighet som har ansvar för att kontrollera att den verksamhet som är under tillsyn lever upp till de krav som ställs på verksamheten. |
| **Tröskelvärde** | Fastställda värden som när de överstigs kan ge indikation på en incident. |
| **Tvåfaktorautentisering** | Metod för åtkomstkontroll, där autentisering bekräftas genom kombination av två olika komponenter. |
| **Validering** | Kontroll och bekräftelse av att något är eller fungerar korrekt. |
| **Verifiering** | Bestyrka riktigheten av något. |
| **VoIP (Voice over IP)** | Röstkommunikation över internetprotokollet IP. |

| Datum: 2020-03-18 | **EXEMPEL Kontakt- och rapporteringsytor vid it-incident eller störning** | | |
|---|---|---|---|
| **Myndighet/aktör:** | Myndigheten för samhällsskydd och beredskap (MSB) | **Myndighet/aktör:** | |
| **Vem?** | IT-incident för samhällsviktiga tjänster, samt vissa digitala tjänster. Regleras i lag 2018:1174 och förordning 2018:1175.<br>Se www.msb.se/nis för mer information. | **Vem?** | |
| **När?** | Rapportera enligt NIS – tre skeenden:<br>1. **Inom sex timmar efter att incident upptäckts.** Sker via telefon.<br>2. **Inom 24 timmar.** Rapport skickas med rekommenderat brev.<br>3. **Inom fyra veckor.** Rapport skickas med rekommenderat brev.<br>Hur rapportering sker se msb.se/nis. | **När?** | |
| **Telefonnummer:** | 010-240 40 40 | **Telefonnummer:** | |
| **E-post:** | cert@cert.se<br>fraga.nis@msb.se | **E-post:** | |
| **Adress:** | CERT-SE<br>MSB<br>Terminalvägen 14<br>171 73 Solna | **Adress:** | |

| Datum: | Kontakt- och rapporteringsytor vid it-incident eller störning | | |
|---|---|---|---|
| **Myndighet/aktör:** | | **Myndighet/aktör:** | |
| **Vem?** | | **Vem?** | |
| **När?** | | **När?** | |
| **Telefonnummer:** | | **Telefonnummer:** | |
| **E-post:** | | **E-post:** | |
| **Adress:** | | **Adress:** | |


Myndigheten för
samhällsskydd
och beredskap

**© Myndigheten för samhällsskydd och beredskap (MSB)**
651 81 Karlstad  Tel 0771-240 240  **www.msb.se**
Publ.nr MSB1930 – februari 2022  ISBN 978-91-7927-245-6