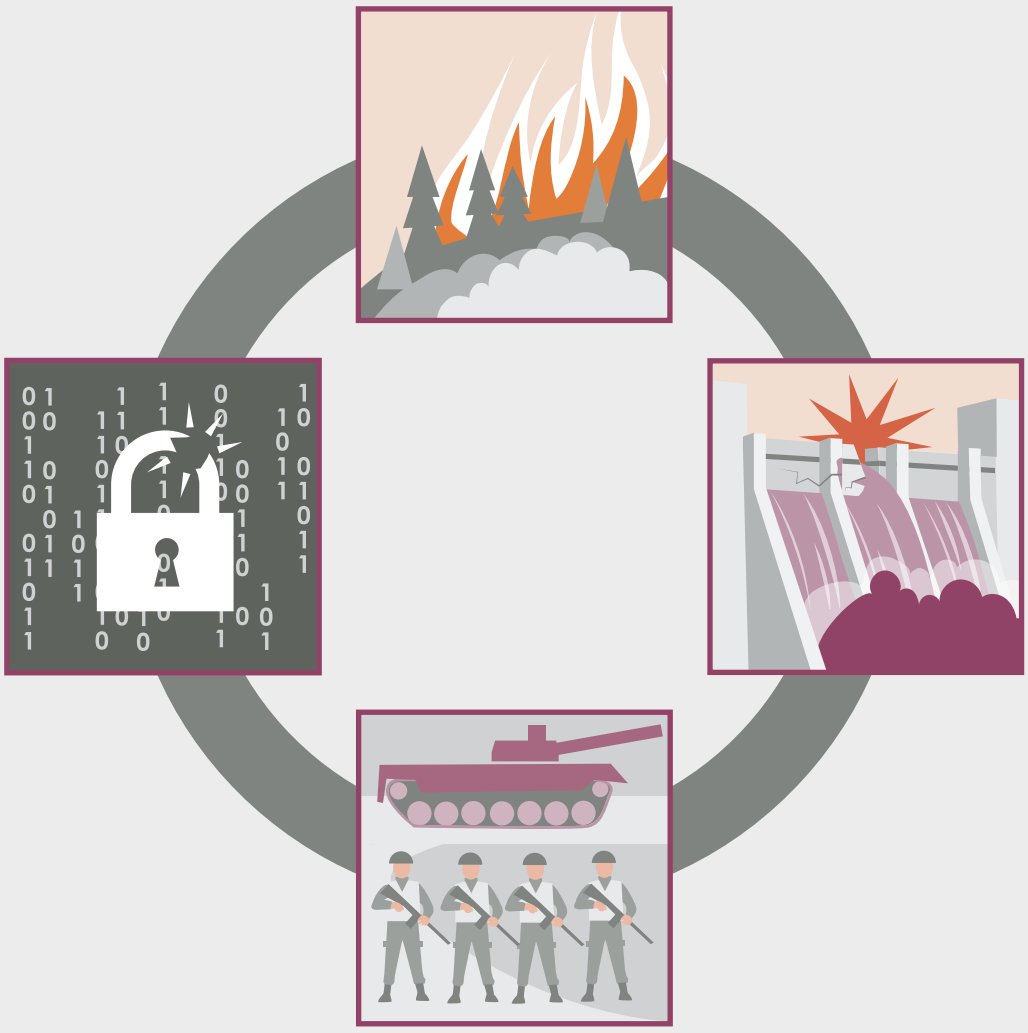
Myndigheten för samhällsskydd och beredskap

VERSION 2 MED ALTERNATIVA SCENARIER

Övning

Informationssäkerhet för ledningen



Övning – Informationssäkerhet för ledningen

Enhet: Enheten för systematisk informationssäkerhet

Produktion: Advant

Publikationsnummer: MSB2228 – reviderad oktober 2024
ISBN: 978-91-7927-552-5

Innehåll

Övningsstöd till organisationer

Inledning

Hur prioriteras informationssäkerhetsåtgärder på kort och lång sikt? Hur vägs informationssäkerhetsrisker mot andra risker i verksamheten? Dessa och andra frågeställningar får organisationens ledning diskutera i denna scenarioövning.

Syftet med övningen är att öva hantering av informationssäkerhetsfrågor i ledningsgruppen genom att belysa utmaningar med att fatta medvetna beslut som behövs för ett riskdrivet systematiskt informationssäkerhetsarbete och skapa underlag för vidare utveckling.

Varför informationssäkerhet?

Vi behöver information för det mesta vi gör, ibland är den till och med livsviktig såsom informationen i patientjournaler eller styrsystemen i kärnkraftverk. Om informationen saknas eller är felaktig kan det få svåra, ibland katastrofala följder. Vi måste skydda vår information så att den alltid finns tillgänglig när vi behöver den, så att vi kan lita på att den är korrekt och inte manipulerad eller förstörd och så att endast behöriga personer får ta del av den. Ett systematiskt förebyggande arbete med informationssäkerhet är viktigt för att säkerställa skyddet av organisationens information, effektivt och över tid. Syftet är att öka kvaliteten och förtroendet i sin verksamhet genom att minska risken för och konsekvenserna av störningar.

Varför ledningen?

Organisationens ledning har en central roll för att det förebyggande arbetet ska fungera. Ledningen ansvarar för att styra och inrikta informationssäkerhetsarbetet, att det är ändamålsenligt organiserat och har adekvata resurser, samt att informationssäkerhetsperspektivet vägs in i beslut som berör verksamheten. Ledningen behöver inte vara experter på informationssäkerhet, men precis som på andra områden behövs viss kunskap för att kunna fatta lämpliga beslut. Personer i ledande befattningar är också viktiga förebilder för den övriga organisationen.

Varför öva?

Övning är ett sätt att öka både medvetenhet och kunskap om ett ämne. Genom att träna på att hantera olika frågeställningar som kan uppstå stärker ledningsgruppen sin förmåga att leda och styra informationssäkerhetsarbetet, vilket alltså i sin tur stärker organisationens informationssäkerhet. Övningar handlar ofta om krishantering vid akuta händelser. Den här övningen tar istället sikte på utmaningar i det löpande arbetet, som om de inte hanteras på ett genomtänkt sätt kan utvecklas till kriser. Fokus är på ledningsperspektivet, alltså den typ av frågeställningar som kan uppstå på ledningsgruppsnivå eller där ledningsgruppen behöver ge verksamheten styrning i en uppkommen situation.

Användning

Dokumentet beskriver ett övningsupplägg kring informationssäkerhet för ledningsgrupper, och hur det kan genomföras. Det riktar sig i första hand till en informationssäkerhetssamordnare eller motsvarande roll eller funktion som planerar och genomför övningen med ledningsgruppen.

Förmågor och scenario

Övningspaketet är inriktat mot generella mål (förmågor) inom informationssäkerhetsarbetet, vilket gör att övningens scenario, och vid behov även inspelen, kan anpassas utifrån organisationens förutsättningar och behov. Tre varianter av övningsscenariet finns som bilagor, utgå ifrån det som passar er verksamhet bäst.

Utvärdering

I övningsstödet ingår färdiga utvärderingsfrågor som med fördel kan kompletteras med egna framtagna. Det medföljer även en mall för utvärderingsrapport som underlag till dokumentation efter genomförd övning. I rapportformatet finns också utrymme att dokumentera relevanta aktiviteter som identifierats för att vidareutveckla organisationens informationssäkerhetsarbete (eller bibehålla det på en lämplig nivå).

Begrepp

Diskussionsledare: Den person som leder och koordinerar planering och genomförande av övningen. Har det övergripande ansvaret för att planera och genomföra övningen inklusive utvärdering och erfarenhetshantering. Diskussionsledaren äger tiden under dagen och är den som medger ev. förändringar.

Utvärderingsledare: Om möjligt är det bra att ha hjälp av en person under övningen, som observerar och dokumenterar förloppet. Denna person har i så fall en viktig del i utvärderingsarbetet efteråt, och kallas i det följande för utvärderingsledare.

Seminarieövning: En seminarieövning kan beskrivas som att spelledaren leder diskussioner med de övande kring en viss frågeställning eller ett scenario. Seminarieövningen karaktäriseras av att övningsdeltagarna tillsammans går igenom eller diskuterar hur de vill/kan lösa eller hantera olika typer av problem eller uppgifter.

Beställare: Den person i ledningsgruppen som agerar mottagare och ansvarar för övningen.

CISO: Förkortning för Chief Information Security Officer. Begreppet används generellt för den som ansvarar för att driva och samordna informationssäkerhetsarbetet i en organisation, oavsett titel.

Moment: Övningens händelser får olika konsekvenser och dessa kallas för moment.

Inspel: De övergripande frågorna som ska diskuteras och som är kopplade till respektive moment.

Utvärdering: Består i att ta reda på och dokumentera hur det går i övningen. Utvärderingen består av två delar, som vägs samman och ligger till grund för utvärderingen.

Erfarenhetshantering: De utvecklingsområden som utgör underlag till åtgärdsrapporten efter avslutad övning.

Läsanvisningar

Som komplement till detta dokument kan man med fördel läsa *Metodhäfte – seminarieövning* för ytterligare vägledning kring utformning och genomförande av övningen: https://www.msb.se/sv/publikationer/ovningsvagledning--metodhafte--seminarieovning/.

För övergripande information och vägledning om övningar finns också *Grundbok – introduktion till och grunder i övningsplanering*: https://www.msb.se/sv/publikationer/ovningsvagledning--grundbok--introduktion-till-och-grunder-i-ovningsplanering/.

Användarinstruktion

Om övningen

Övningen vänder sig i första hand till ledningsgrupper och riktar sig till alla typer av verksamheter. Det scenario som används för genomförandet finns i tre varianter, bilagda i slutet av handledningen. Bilaga A riktar sig till kommun och region. Bilaga B riktar sig till företag och bilaga C statliga myndigheter och andra organisationer.

Genom samtal och diskussion utvecklas deltagarna i förmågor rörande ledningens roll i informationssäkerhetsarbetet. Utifrån övningens scenario presenteras frågeställningar och inspel för deltagarna. Diskussionsledaren ansvarar för att leda diskussionerna i en riktning så att syftet med övningen uppnås.

Att genomföra övningen beräknas ta 90 minuter, men tiden är ungefärlig och beror bland annat på hur mycket som kommer att ändras i scenariot. Se vidare i övningsbestämmelserna nedan.

Förberedelser

Exempel på förberedelseåtgärder kan vara uppdragsdialog med beställaren (den person i ledningsgruppen som agerar mottagare och ansvarar för övningen) där syfte och mål klargörs samt hur erfarenheter från övningen ska hanteras.

- **Behovsanalys:** Hur ser nuläget ut, ur ledningsgruppens perspektiv? Vilka förkunskaper har de? Finns det aktuella omständigheter i eller kring organisationen som kan vara relevanta? Vilka förväntningar finns från de olika parterna?
- **Syfte och mål med övningen.**
- **Scenariotema:** Fungerar det befintliga scenariot, hur kan det utvecklas och eventuellt anpassas?
- **Resurser:** Vem förbereder och genomför övningen? Vilka personer deltar?
- **Roller och ansvar under övningen:** Viktigt att diskussionsledarens roll och mandat är tydligt.
- **När och var ska övningen äga rum:** Inom ramen för befintligt möte? Separat tillfälle?
- **Hur ska erfarenheterna från övningen hanteras och vem är ansvarig (beställaren!).**

Det viktigaste i all övningsverksamhet är erfarenhetshanteringen. Före övningen ska beställaren och genomföraren vara överens om vad som är syftet med övningen och utvärderingen, hur utvärderingen ska redovisas och hur eventuella förändringar ska omhändertas i organisationen.

Förmöte med ledningsgruppen

Beroende på organisationens mognad och ledningsgruppens förkunskaper på informationssäkerhetsområdet kan det vara lämpligt att kombinera övningen med en utbildningsaktivitet, till exempel en grundläggande orientering om ämnet, en genomgång av aktuellt läge eller nya omständigheter som påverkar organisationens informationssäkerhetsarbete. Förslagsvis kan detta göras innan övningstillfället, det fungerar då i att förbereda deltagarna för diskussionerna samtidigt som övningen kan bidra till att stärka utbildningsaktiviteten.

Under övningen

Övningsscenariot finns i tre varianter, bilagda i slutet av handledningen. Använd det som passar er verksamhet bäst.

Först introduceras scenariot. Det utvecklas sedan stegvis genom tre moment med nya händelser. Inspelen som är kopplade till varje moment innehåller ett antal frågor som diskussionsledaren spelar in och sedan låter deltagarna diskutera. Om deltagarna inte är färre än 4 bör de diskutera i två grupper vid de olika momenten. Detta för att bättre belysa olika sätt att resonera och svara på frågorna, och få en större bredd i olika perspektiv och synsätt som vägs in.

Uteblir diskussionen, eller om diskussionsledaren känner att man vill fördjupa och ”spetsa till” diskussionerna, finns ett antal understödjande frågor.

Anteckna huvudpunkter från de olika diskussionerna på tavla, blädderblock eller liknande för att underlätta kopplingar mellan moment. Efter de tre momenten kommer en sammanfattande diskussion med hela gruppen kring några frågeställningar som kopplas till målen med övningen.

Avslutningsvis får deltagarna svara på några frågor för att utvärdera övningen.

Efter övningen

Som stöd för utvärderingsarbetet medföljer mallar för utvärdering med ett antal frågeställningar. Det finns även utrymme att fylla på med egna utvärderingsfrågor utifrån eventuella egna delsyften och delmål. Både deltagarna och diskussionsledare/utvärderingsledare utvärderar övningen.

Det medföljer även en mall för utvärderingsrapport, som hjälp för att skapa en systematik i övningsutvärderingen och för att omsätta erfarenheterna i förändringar och förbättringar. Slutsatserna ska också föda in till det löpande systematiska arbetet med informationssäkerhet i organisationen. Det är viktigt att utvärderingsrapporten återkopplas till beställaren (den person i ledningsgruppen som agerar mottagare och ansvarar för övningen) och att planen framåt förankras i ledningsgruppen.

Lycka till!

Övningsbestämmelser för genomförande

Övningens namn: *Att styra informationssäkerhetsarbetet – vi kom, vi såg, vi säkrade.*

Datum och tid för övningens genomförande:

Syfte: Att öva hantering av informationssäkerhetsfrågor för ledningsgruppen genom att belysa utmaningar med att fatta medvetna beslut som behövs för ett riskdrivet systematiskt informationssäkerhetsarbete.

Mål:

1. Identifiera åtgärder eller beslut som behöver fattas på kort respektive längre sikt.
2. Efterfråga informationssäkerhetsaspekter i beslutsunderlag.
3. Väga informationssäkerhetsrisker mot andra risker och mål.

Målgrupp: Ledningsgrupp.

Förkunskaper: Kännedom om den egna organisation och översiktligt om dess informationssäkerhetsarbete. Läst igenom publikationen *Ledningens roll inom informationssäkerhet – Stöd för dig med en ledande funktion*: https://www.msb.se/sv/publikationer/ledningens-roll-inom-informationssakerhet---stod-for-dig-med-en-ledande-funktion/.

Det är en fördel att även ha kännedom om aktuell riskanalys, organisationens dataskyddsarbete och andra relevanta lagkrav, nationella och regionala strategier samt aktuella omvärldsfaktorer, exempelvis krav från uppdragsgivare, utveckling i branschen m.m.

Format: Seminarieövning.

Övningsledning: Diskussionsledare (ansvarar för att leda diskussionerna i en riktning så att syftet med övningen uppnås). Diskussionsledaren äger tiden under dagen och är den som medger ev. förändringar.

Tid för förberedelse: Uppskattningsvis minst 4–6 tim.

Tid för genomförande: ca 90 min.

Tid för utvärdering: 30 min.

Logistik: Se checklista på nästa sida.

Checklista för genomförande

Checklista för genomförande av seminarieövning

- [ ] Genomför uppdragsdialog där förutsättningar, datum och tid gås igenom med beställaren.
- [ ] Boka övningslokal med nödvändig utrustning.
- [ ] Boka in och förbered eventuellt förmöte med deltagarna.
- [ ] Boka och bjud in deltagarna till övningen.
- [ ] Anpassa övningsscenariot utifrån den egna organisationen.
- [ ] Förbered presentationsmaterial och andra dokument.
- [ ] Förbered dokumentation och utvärdering (inklusive återkoppling).
- [ ] Vid behov, förbered övningslokal och andra praktiska detaljer.
- [ ] Gå igenom inspelen och de understödjande frågorna så att diskussionsledaren är väl förberedd inför genomförandet.
- [ ] Genomför övningen och låt deltagarna fylla i utvärderingsformulär.
- [ ] Skriv utvärderingsrapport (utvärderingsledaren är ansvarig).
- [ ] Gå igenom erfarenheterna från övningen, planera hur de ska tas om hand och hur arbetet ska följas upp.

Förslag tidsupplägg

Tid	Innehåll
09:00–09:05	Presentera övningen och gå igenom övningsbestämmelserna
09:05–09:25	Moment 1
09:25–09:45	Moment 2
09:45–10:05	Moment 3
10:05–10:20	Sammanfattande diskussion
10:20–10:30	Utvärdering och erfarenhetshantering

Scenario och händelser

Genomför övningen med utgångspunkt i ert valda och eventuellt anpassade scenario. Övningsdeltagarna utgör ledningsgruppen och det har tidigare skett ett intrång i ett administrativt system. Intrånget innebär att information hämtades ut men sårbarheten som nyttjades är nu åtgärdad och systemet åter i drift.

Scenariot utvecklas i den första händelsen där det framkommer att det finns brister i informationssäkerheten. Genom inspel till momentet får deltagarna ytterligare förutsättningar att förhålla sig till när de sedan ska reflektera över och diskutera hur de hanterar konsekvenserna av de identifierade bristerna.

Nästa moment innebär ytterligare utmaningar genom att den medarbetare som är ansvarig för att driva informationssäkerhetsfrågorna blir sjukskriven. Inspelen beskriver omständigheterna kring sjukskrivningen och deltagarna får ta ställning till vad detta innebär för det fortsatta informationssäkerhetsarbetet.

I det tredje och avslutande momentet upptäcks sårbarheter i ett verktyg som används för att genomföra en viktig del av verksamheten. Riktigheten för informationen som hanteras kan inte längre garanteras. Inspelen ger deltagarna inriktning till att diskutera risker utifrån olika perspektiv och hur konsekvenserna ska hanteras.

Varje moment innehåller en diskussion där övningsdeltagarna reflekterar över innebörden i de förutsättningar som scenariot presenterar i mindre grupper. Slutsatserna från gruppdiskussionerna redovisas sedan gemensamt.

Välj det scenario som motsvarar er verksamhet från bilagorna

Bilaga A. Grundscenario för kommun och region

Bilaga B. Grundscenario för företag

Bilaga C. Grundscenario för statliga myndigheter och andra organisationer

Utvärderingsenkät

Enkäten syftar till att de övande ska självskatta i vilken utsträckning övningen har uppfyllt definierat syfte och mål. Anpassningar kan vid behov göras i utvärderingsenkäten. Utvärderingsenkäten besvaras av deltagarna vid övningens slut och ligger till grund för resultatets analys och för utvärderingsrapporten. Frågorna kan besvaras på papper, via mentimeter eller på annat sätt.

Namn: _____

Roll: _____

Nr	Fråga	Mycket stor utsträckning	Stor utsträckning	Liten utsträckning	Inte alls
1.	Uppnåddes syftet? *Belysa utmaningar med att fatta medvetna beslut som behövs för ett riskdrivet systematiskt informationssäkerhetsarbete.*	☐	☐	☐	☐
2.	Har ledningsgruppen tillräcklig förmåga att fatta lämpliga beslut för informationssäkerhetsarbetet (åtgärder som behövs på kort och lång sikt, efterfråga beslutsunderlag, väga olika risker mot varandra)?	☐	☐	☐	☐
3.	Har diskussionen visat på brister i organisationens förmåga att stödja ledningsgruppens arbete enligt ovan?	Fritextsvar:			
4.	Vilka aktiviteter och/eller förändringar behövs?	Fritextsvar:			
5.	Reflektioner kring övningens innehåll och genomförande?	Fritextsvar:			

Utvärderingsrapport

Rapport för stödjandeseminarieövning med fokus på aktörs-gemensam inriktning och samordning

Organisation:

Datum:

Datum för övningens genomförande:

Bakgrund

Organisationens ledning har en central roll för att det förebyggande arbetet ska fungera. Ledningen ansvarar för att styra och inrikta informationssäkerhetsarbetet, att det är ändamålsenligt organiserat och har adekvata resurser, samt att informationssäkerhetsperspektivet vägs in i beslut som berör verksamheten. Ledningen behöver inte vara experter på informationssäkerhet, men precis som på andra områden behövs viss kunskap för att kunna fatta lämpliga beslut.

Övning är ett sätt att öka både medvetenhet och kunskap om ett ämne. Genom att träna på att hantera olika frågeställningar som kan uppstå stärker ledningsgruppen sin förmåga att leda och styra informationssäkerhetsarbetet, vilket alltså i sin tur stärker organisationens informationssäkerhet. Övningen tog sikte på utmaningar i det löpande arbetet, som om de inte hanteras på ett genomtänkt sätt kan utvecklas till kriser. Fokus var på ledningsperspektivet, alltså den typ av frågeställningar som kan uppstå på ledningsgruppsnivå eller där ledningsgruppen behöver ge verksamheten styrning i en uppkommen situation.

Beskrivning av övningen

Format: Seminarieövningen med fokus på informationssäkerhetsfrågor genomfördes genom samtal och diskussion.

Syfte: Belysa utmaningar med att fatta medvetna beslut som behövs för ett riskdrivet systematiskt informationssäkerhetsarbete och skapa underlag för vidare utveckling.

Metod: Utifrån nedanstående mål skapades ett antal inspel och frågor som möjliggjorde för deltagarna att genom diskussion och analyser nå de uppsatta målen för övningen. Diskussionen leddes av en diskussionsledare som hade inspel och understödjande frågor till sin hjälp för att lotsa deltagarna mot målen.

[Justera utifrån om en utvärderingsledare medverkar eller ej]

Diskussionen observerades och dokumenterades av utvärderingsledaren. Alternativt: Huvudpunkter i diskussionen dokumenterades under övningen (anpassa utifrån hur diskussionen dokumenterats).

Detta, tillsammans med deltagarnas utvärderingar, ligger till grund för denna rapport.

Mål:

1. Identifiera åtgärder eller beslut som behöver fattas på kort respektive längre sikt.
2. Efterfråga informationssäkerhetsaspekter i beslutsunderlag.
3. Väga informationssäkerhetsrisker mot andra risker och mål.

Övningsdeltagare

(Övningsansvarig fyller i namn och roll i ledningsgruppen i nedanstående tabell.)

Roll	Namn

Utvärderingsmetod

Utvärderingen bestod i att ta reda på och dokumentera hur det gick i övningen och vilka utvecklingsområden som identifierades. Utvärderingen bestod av två delar, en självskattande del som de övande själva genomförde efter avslutad övning via en enkät, och en andra del där ansvarig utvärderare följde de övande under övningen och noterade diskussioner och slutsatser i förhållande till målen. Dessa två underlag har sedan vägts samman och legat till grund för utvärderingen.

Resultat från övningen

(Lägg in det sammanställda resultatet från analysen av diskussioner och utvärderingar under respektive mål och rubrik nedan.)

1. **Ledningsgruppen identifierar åtgärder eller beslut som behöver fattas på kort respektive längre sikt.**

   Viktiga punkter från diskussionerna:

   Viktiga punkter från deltagarnas utvärderingar:

2. **Ledningsgruppen efterfrågar informationssäkerhetsaspekter i beslutsunderlag.**

   Viktiga punkter från diskussionerna:

   Viktiga punkter från deltagarnas utvärderingar:

3. **Ledningsgruppen väger informationssäkerhetsrisker mot andra risker och mål.**

   Viktiga punkter från diskussionerna:

   Viktiga punkter från deltagarnas utvärderingar:

Förbättringsområden och vidare arbete

Beskriv slutsatser och rekommendationer utifrån sammanställningen, samt de åtgärder som bör genomföras för att nå högre insikt och kunskap. Rekommendationerna kan skrivas i punktform och motiveras med fritext. De åtgärder som behöver genomföras för att uppnå rekommendationerna bryts ned och noteras i nedanstående åtgärdsplan. Det är viktigt att här göra en koppling till det löpande systematiska arbetet med informationssäkerhet i organisationen.

Gå igenom rapporten med beställaren och presentera resultatet i ledningsgruppen.

Slutsatser och rekommendationer

Åtgärdsplan

Nr	Förbättringsområden	Åtgärd	Ansvarig (namn)	Genomförande (datum)	Åtgärd senast (datum)	Uppföljning av åtgärd (datum)
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						

Bilaga A. Grundscenario för kommun och region

Bakgrund till scenario

Här kan du lägga till relevant information utifrån er kommun eller region. För att öka igenkänningen kan ni specificera vilket administrativt system som drabbats eller referera till ett aktuellt projekt.

Förhistoria

Övningen utgår ifrån er egen organisation, där övningsdeltagarna utgör ledningsgruppen.

Organisationen utsattes under sommaren för ett intrång i ett administrativt system och information från databasen hämtades ut. Sårbarheten som nyttjades är nu åtgärdad och systemet är åter i drift. Händelsen har dock blottlagt brister i vårt informationssäkerhetsarbetet.

Momentbeskrivning 1

Återrapportering från arbetet med intern uppföljning

Tidsförhållanden

Presentera uppgiften: 5 min.

Arbeta med inspelen 1–3: 10 min.

Redovisa svaret: 5 min.

Total tid för momenten: ca 20 min.

Aktörer

Samtliga deltagare, indelade i två eller flera grupper om 2–4 personer för diskussion kring inspelsfrågorna.

Händelse

På ledningsgruppsmötet presenteras resultatet av en intern uppföljning av informationssäkerheten i den verksamhet som hanterar kommunen eller regionens mest värdefulla information. Rapporten visar att det förebyggande arbetet har stora brister.

Inspel

Bristerna som identifierats i uppföljningen är följande:

a. Trots att roller och ansvar finns reglerat i styrdokument så brister informationsägarna i sitt ansvar, bland annat genom att inte återkommande revidera och uppdatera informationsklassningarna.

b. Det visar sig även att det fortfarande saknas fastställda klassningar i flera delprocesser.

c. Detta har lett till att kommunens/regionens medarbetare inte följer de hanteringsanvisningar som följer av informationsklassningen.

d. Flera av medarbetarna uppgav att de inte känner till dessa eller var man hittar dem.

e. Några har också uppgett att de inte lägger så mycket fokus på detta då ”systemen är uppsatta så att det inte går att göra fel”.

f. Uppföljningen har resulterat i följande förslag på åtgärder:

- tydliggör roller och ansvar
- stärk uppföljningen på området
- återkommande utbildning till medarbetarna.

De interna bristerna innebär risker för möjligheten att bedriva samhällsviktig verksamhet. På ledningsgruppsmötet vill ni inrikta organisationens säkerhetskultur. Ni inser att det är både ett långsiktigt och kortsiktigt arbete.

Diskussionsfrågor:

1.1. Hur prioriterar ni arbetet med anledning av resultatet från uppföljningen? (långsiktigt kontra kortsiktigt)

1.2. Vad är viktigast för er och varför?

1.3. Vilken säkerhetskultur vill ni ha? Hur går ni tillväga?

1.4. Vilka beslut fattar ni?

Understödjande frågor

Frågorna kan användas av diskussionsledaren i samband med gruppernas redovisning (anpassa efter gruppens mognad och hur diskussionen utvecklas):

- Vilka utmaningar såg ni?
- Hur resonerade ni kring de förutsättningar som behöver vara på plats för besluten ni fattat?
- Koppla tillbaka till de åtgärdsförslag som presenterades från uppföljningen – hur adresserades de?
- Hur kommunicerar ni kring den lösning ni valt?

Momentbeskrivning 2

Informationssäkerhetssamordnaren blir långtidssjukskriven

Tidsförhållanden

Presentera uppgiften: 5 min.

Arbeta med inspelen 1–3: 10 min.

Redovisa svaret: 5 min.

Total tid för momenten: ca 20 min.

Aktörer

Samtliga deltagare, indelade i två eller flera grupper om 2–4 personer för diskussion kring inspelsfrågorna.

Händelse

Tre veckor senare blir den medarbetare som samordnar arbetet med informationssäkerhet (informationssäkerhetssamordnare, ”CISO” eller motsvarande) i er kommun eller region hastigt långtidssjukriven.

Inspel

Kommunens/regionens informationssäkerhetssamordnare har hastigt blivit långtidssjukskriven på heltid minst sex månader och kommer därefter troligen att vara deltidssjukskriven ytterligare sex månader.

Informationssäkerhetssamordnaren utgör en viktig kugge i er säkerhetsorganisation och har ansvar för en stor del av förbättringsåtgärderna som föreslagits i uppföljningen.

Förutom att ha ett ansvar för att driva igenom de beslut som ni just tagit så är er informationssäkerhetssamordnare också ett viktigt stöd för er informationshantering vid flytten till nya kontorslokaler, som ska vara genomförd om nio månader.

Diskussionsfrågor:

2.1. Vilka risker innebär detta för organisationens långsiktiga informationssäkerhetsarbete?

2.2. Hur väljer ni att lösa den uppkomna utmaningen ur ett kontinuitetsperspektiv?

Understödjande frågor

Frågorna kan användas av diskussionsledaren i samband med gruppernas redovisning (anpassa efter gruppens mognad och hur diskussionen utvecklas):

- Vilka utmaningar såg ni?
- Hur resonerade ni kring de förutsättningar som behöver vara på plats för den lösning ni valt?
- Koppla tillbaka till frågorna – vilka risker ser ni? Vilka åtgärder vidtar ni för att säkerställa kontinuiteten?
  - Vad har de svarat, tas med till nästa moment (ex riskerna).
- Hur kommunicerar ni kring den lösning ni valt?
- Har det skett någon förändring från förra momentet? Påverkas situationen av det som hände nu, och i så fall hur?

Momentbeskrivning 3

Nytt digitalt verktyg i verksamheten

Tidsförhållanden

Presentera uppgiften: 5 min.

Arbeta med inspelen 1–3: 10 min.

Redovisa svaret: 5 min.

Total tid för momenten: ca 20 min.

Aktörer

Samtliga deltagare, indelade i två eller flera grupper om 2–4 personer för diskussion kring inspelsfrågorna.

Händelse

Sex månader senare inför organisationen ett nytt digitalt verktyg för en central process i verksamheten.

Inspel

Anpassa beskrivningen så att det blir konkret och realistiskt för er organisation!
Medarbetare som jobbar i samhällsviktig verksamhet behöver både ta del av information och kunna dokumentera verksamheten. Informationen är nödvändig för att kunna utföra verksamheten. Dessutom är informationen känslig. Verksamheten är beroende av att verktyget fungerar dygnet runt.

Verktyget har varit i drift en tid då det upptäcks att det har en sårbarhet som kan leda till att riktigheten i informationen inte kan garanteras.

Diskussionsfrågor:

3.1. Vilka risker ser ni på kort respektive lång sikt?

3.2. Hur väljer ni att hantera dessa risker?

3.3. För att kunna hantera riskerna – vilken typ av frågor/uppdrag ställer ni till ansvarig i er organisation?

3.4. Vem/vilka i er organisation är ansvarig/a?

Understödjande frågor

Frågorna kan användas av diskussionsledaren i samband med gruppernas redovisning (anpassa efter gruppens mognad och hur diskussionen utvecklas):

- Vilka utmaningar såg ni?
- Hur resonerade ni kring förtroenderiskerna?
- Vilken roll har det främsta mandatet att agera?
- Hur kommunicerar ni kring den lösning ni valt?
- Har det skett någon förändring från förra momentet? Påverkas situationen av det som hände nu, och i så fall hur?

Sammanfattande diskussion

Tidsförhållanden

Total tid för momentet: ca 15 min.

Aktörer

Gemensam diskussion med samtliga deltagare.

Diskussionsfrågor

Vad tar ni med er från dagens diskussion avseende:

- Hur ledningen påverkar arbetet, kortsiktigt och långsiktigt.
- Utmaningar med att skapa och upprätthålla en säkerhetskultur.
- Informationssäkerhetsaspekter (riskanalyser) som en del av frågor inom andra områden, både i det dagliga arbetet och vid händelser.
- Informationssäkerhetsrisker i förhållande till andra risker och mål.

Diskussionsledaren avrundar och berättar om hur erfarenhetshanteringen kommer att gå till. Varje deltagare får svara på utvärderingsfrågorna innan passet avslutas.

Bilaga B. Grundscenario för företag

Bakgrund till scenario

Här kan du lägga till relevant information utifrån ert företag. För att öka igenkänningen kan ni specificera vilket administrativt system som drabbats eller referera till ett aktuellt projekt.

Förhistoria

Övningen utgår från ert företag, där övningsdeltagarna utgör ledningsgruppen.

Ert företag utsattes under sommaren för ett intrång i ett administrativt system och information från databasen läckte ut. Sårbarheten som nyttjades är nu åtgärdad och systemet är åter i drift.

Momentbeskrivning 1

Återrapportering från internrevisionen

Tidsförhållanden

Presentera uppgiften: 5 min.

Arbeta med inspelen 1–3: 10 min.

Redovisa svaret: 5 min.

Total tid för momenten: ca 20 min.

Aktörer

Samtliga deltagare, indelade i två eller flera grupper om 2–4 personer för diskussion kring inspelsfrågorna.

Händelse

På ledningsgruppsmötet presenteras en rapport från internrevisionen angående informationssäkerheten. Rapporten visar på stora brister i det förebyggande arbetet, inklusive i den del av företaget som hanterar information som behövs för att tidskritisk verksamhet ska kunna bedrivas utan störningar.

Inspel

Bristerna som identifierats i internrevisionen är följande:

a. Trots att roller och ansvar finns reglerat i företagets styrande dokument så brister informationsägarna i sitt ansvar, bland annat att inte återkommande revidera och uppdatera riskanalyser som ska säkerställa att rätt åtgärder vidtas.

b. Det visar sig även att det fortfarande saknas fastställda klassningar i flera affärskritiska delprocesser.

c. Detta har lett till att företagets medarbetare inte följer anvisningar och rutiner som följer av informationsklassningen.

d. Flera av medarbetarna uppgav att de inte känner till dessa eller var man hittar dem.

e. Några har också uppgett att de inte lägger så mycket fokus på detta då ”systemen är uppsatta så att det inte går att göra fel”.

f. Internrevisionen har lämnat följande förslag på åtgärder:

- tydliggör roller och ansvar
- stärk uppföljningen på området
- återkommande utbildning till medarbetarna.

De interna bristerna innebär risker för företagets leveranser. På ledningsgruppsmötet vill ni hantera bristerna och inrikta företagets säkerhetskultur. Ni inser att det är både ett långsiktigt och kortsiktigt arbete.

Diskussionsfrågor:

1.1. Hur prioriterar ni arbetet med anledning av internrevisionens rapport? (långsiktigt kontra kortsiktigt)

1.2. Vad är viktigast för er och varför?

1.3. Vilken säkerhetskultur vill ni ha? Hur går ni tillväga?

1.4. Vilka beslut fattar ni?

Understödjande frågor

Frågorna kan användas av diskussionsledaren i samband med gruppernas redovisning (anpassa efter gruppens mognad och hur diskussionen utvecklas):

- Vilka utmaningar såg ni?
- Hur resonerade ni kring de förutsättningar som behöver vara på plats för besluten ni fattat?
- Koppla tillbaka till internrevisionens åtgärdsförslag – hur adresserades de?
- Hur kommunicerar ni kring den lösning ni valt?

Momentbeskrivning 2

CISO blir långtidssjukskriven

Tidsförhållanden

Presentera uppgiften: 5 min.

Arbeta med inspelen 1–3: 10 min.

Redovisa svaret: 5 min.

Total tid för momenten: ca 20 min.

Aktörer

Samtliga deltagare, indelade i två eller flera grupper om 2–4 personer för diskussion kring inspelsfrågorna.

Händelse

Tre veckor senare blir företagets CISO eller motsvarande (informationssäkerhetschef eller motsvarande roll med ansvar för att driva och samordna informationssäkerhetsarbetet) hastigt långtidssjukskriven.

Inspel

Företagets CISO har blivit långtidssjukskriven på heltid minst sex månader och kommer därefter troligen att vara deltidssjukskriven ytterligare sex månader.

CISO:n utgör en viktig kugge i er säkerhetsorganisation och har ansvar för företagets informationssäkerhetsstrategi och ska driva en stor del av förbättringsåtgärderna som internrevisionen föreslagit.

Förutom att ha ett ansvar för att driva igenom de beslut som ni just tagit så är er CISO också en garant för er informationshantering vid flytten av huvudkontoret till nya lokaler, som ska vara genomförd om nio månader.

Diskussionsfrågor:

2.1. Vilka risker innebär detta för företagets långsiktiga informationssäkerhetsarbete?

2.2. Hur väljer ni att lösa den uppkomna utmaningen ur ett kontinuitetsperspektiv?

Understödjande frågor

Frågorna kan användas av diskussionsledaren i samband med gruppernas redovisning (anpassa efter gruppens mognad och hur diskussionen utvecklas):

- Vilka utmaningar såg ni?
- Hur resonerade ni kring de förutsättningar som behöver vara på plats för den lösning ni valt?
- Koppla tillbaka till frågorna – vilka risker ser ni? Vilka åtgärder vidtar ni för att säkerställa kontinuiteten?
  - Vad har de svarat, tas med till nästa moment (ex riskerna).
- Hur kommunicerar ni kring den lösning ni valt?
- Har det skett någon förändring från förra momentet? Påverkas situationen av det som hände nu, och i så fall hur?

Momentbeskrivning 3

Nytt verktyg för rapportering

Tidsförhållanden

Presentera uppgiften: 5 min.

Arbeta med inspelen 1–3: 10 min.

Redovisa svaret: 5 min.

Total tid för momenten: ca 20 min.

Aktörer

Samtliga deltagare, indelade i två eller flera grupper om 2–4 personer för diskussion kring inspelsfrågorna.

Händelse

Sex månader senare inför företaget ett nytt IT-system för en central process i verksamheten.

Inspel

Anpassa beskrivningen så att det blir konkret och realistiskt för er organisation!
Medarbetare som jobbar i ett viktigt uppdrag behöver ta del av information och dokumentera verksamheten dygnet runt. Tillgång till korrekt information är nödvändig för att kunna utföra verksamheten. Dessutom är informationen känslig och får inte hamna i fel händer. Det är också

Verktyget har varit i drift en tid då det upptäcks att det har en sårbarhet som kan leda till att riktigheten i informationen inte kan garanteras.

Diskussionsfrågor:

3.1. Vilka risker ser ni på kort respektive lång sikt?

3.2. Hur väljer ni att hantera dessa risker?

3.3. För att kunna hantera riskerna – vilken typ av frågor/uppdrag ställer ni till ansvarig i ert företag?

3.4. Vem/vilka i ert företag är ansvarig/a?

Understödjande frågor

Frågorna kan användas av diskussionsledaren i samband med gruppernas redovisning (anpassa efter gruppens mognad och hur diskussionen utvecklas):

- Vilka utmaningar såg ni?
- Hur resonerade ni kring förtroenderiskerna?
- Vilken roll har det främsta mandatet att agera?
- Hur kommunicerar ni kring den lösning ni valt?
- Har det skett någon förändring från förra momentet? Påverkas situationen av det som hände nu, och i så fall hur?

Sammanfattande diskussion

Tidsförhållanden

Total tid för momentet: ca 15 min.

Aktörer

Gemensam diskussion med samtliga deltagare.

Diskussionsfrågor

Vad tar ni med er från dagens diskussion avseende:

- Hur ledningen påverkar arbetet, kortsiktigt och långsiktigt.
- Utmaningar med att skapa och upprätthålla en säkerhetskultur.
- Informationssäkerhetsaspekter (riskanalyser) som en del av frågor inom andra områden, både i det dagliga arbetet och vid händelser.
- Informationssäkerhetsrisker i förhållande till andra risker och mål.

Diskussionsledaren avrundar och berättar om hur erfarenhetshanteringen kommer att gå till. Varje deltagare får svara på utvärderingsfrågorna innan passet avslutas.

Bilaga C. Grundscenario statliga myndigheter och andra organisationer

Bakgrund till scenario

Här kan du lägga till relevant information utifrån er organisation.

Förhistoria

Övningen utgår ifrån er egen organisation, där övningsdeltagarna utgör ledningsgruppen.

Organisationen utsattes under sommaren för ett intrång i ett administrativt system och information från databasen hämtades ut. Sårbarheten som nyttjades är nu åtgärdad och systemet är åter i drift.

Momentbeskrivning 1

Återrapportering från internrevisionen

Tidsförhållanden

Presentera uppgiften: 5 min.

Arbeta med inspelen 1–3: 10 min.

Redovisa svaret: 5 min.

Total tid för momenten: ca 20 min.

Aktörer

Samtliga deltagare, indelade i två eller flera grupper om 2–4 personer för diskussion kring inspelsfrågorna.

Händelse

På ledningsgruppsmötet presenteras en intern revision av informationssäkerheten i den verksamhet som hanterar organisationens mest värdefulla information. Rapporten visar att det förebyggande arbetet har stora brister.

Inspel

Bristerna som identifierats i internrevisionen är följande:

a. Trots att roller och ansvar finns reglerat i styrdokument så brister informationsägarna i sitt ansvar bland annat att inte återkommande revidera och uppdatera informationsklassningarna.

b. Det visar sig även att det fortfarande saknas fastställda klassningar i flera delprocesser.

c. Detta har lett till att organisationens medarbetare inte följer de hanterings-anvisningar (säkerhetsåtgärder) som följer av informationsklassningen.

d. Flera av medarbetarna uppgav att de inte känner till dessa eller var man hittar dem.

e. Några har också uppgett att de inte lägger så mycket fokus på detta då ”systemen är uppsatta så att det inte går att göra fel”.

f. Internrevisionen har lämnat följande förslag på åtgärder:

- tydliggör roller och ansvar
- stärk uppföljningen på området
- återkommande utbildning till medarbetarna.

På ledningsgruppsmötet vill ni inrikta organisationens säkerhetskultur. Ni inser att det är både ett långsiktigt och kortsiktigt arbete.

Diskussionsfrågor:

1.5. Hur prioriterar ni arbetet med anledning av internrevisionens rapport? (långsiktigt kontra kortsiktigt)
1.6. Vad är viktigast för er och varför?
1.7. Vilken säkerhetskultur vill ni ha? Hur går ni tillväga?
1.8. Vilka beslut fattar ni?

Understödjande frågor

Frågorna kan användas av diskussionsledaren i samband med gruppernas redovisning (anpassa efter gruppens mognad och hur diskussionen utvecklas):

- Vilka utmaningar såg ni?
- Hur resonerade ni kring de förutsättningar som behöver vara på plats för besluten ni fattat?
- Koppla tillbaka till internrevisionens åtgärdsförslag – hur adresserades de?
- Hur kommunicerar ni kring den lösning ni valt?

Momentbeskrivning 2

CISO blir långtidssjukskriven

Tidsförhållanden

Presentera uppgiften: 5 min.

Arbeta med inspelen 1–3: 10 min.

Redovisa svaret: 5 min.

Total tid för momenten: ca 20 min.

Aktörer

Samtliga deltagare, indelade i två eller flera grupper om 2–4 personer för diskussion kring inspelsfrågorna.

Händelse

Tre veckor senare blir organisationens informationssäkerhetsamordnare eller motsvarande (”CISO”) hastigt långtidssjukriven.

Inspel

Organisationens CISO har hastigt blivit långtidssjukskriven på heltid minst sex månader och kommer därefter troligen att vara deltidssjukskriven ytterligare sex månader.

CISO:n utgör en viktig kugge i er säkerhetsorganisation och har ansvar för en stor del av förbättringsåtgärderna som internrevisionen föreslagit.

Förutom att ha ett ansvar för att driva igenom de beslut som ni just tagit så är er CISO också en garant för er informationshantering vid flytten av huvudkontoret till nya lokaler, som ska vara genomförd om nio månader.

Diskussionsfrågor:

2.1. Vilka risker innebär detta för organisationens långsiktiga informationssäkerhetsarbete?

2.2. Hur väljer ni att lösa den uppkomna utmaningen ur ett kontinuitetsperspektiv?

Understödjande frågor

Frågorna kan användas av diskussionsledaren i samband med gruppernas redovisning (anpassa efter gruppens mognad och hur diskussionen utvecklas):

- Vilka utmaningar såg ni?
- Hur resonerade ni kring de förutsättningar som behöver vara på plats för den lösning ni valt?
- Koppla tillbaka till frågorna – vilka risker ser ni? Vilka åtgärder vidtar ni för att säkerställa kontinuiteten?
  - Vad har de svarat, tas med till nästa moment (ex riskerna).
- Hur kommunicerar ni kring den lösning ni valt?
- Har det skett någon förändring från förra momentet? Påverkas situationen av det som hände nu, och i så fall hur?

Momentbeskrivning 3

Nytt verktyg för rapportering

Tidsförhållanden

Presentera uppgiften: 5 min.

Arbeta med inspelen 1–3: 10 min.

Redovisa svaret: 5 min.

Total tid för momenten: ca 20 min.

Aktörer

Samtliga deltagare, indelade i två eller flera grupper om 2–4 personer för diskussion kring inspelsfrågorna.

Händelse

Sex månader senare inför organisationen ett nytt verktyg för en central process i verksamheten.

Inspel

Anpassa beskrivningen så att det blir konkret och realistiskt för er organisation!
Ett antal externa aktörer har skyldighet att rapportera in information om störningar eller andra uppgifter som kan vara känsliga. Både ni och aktörerna är beroende av att verktyget fungerar, och att upprätthålla förtroendet är avgörande för relationen med de externa aktörerna

Verktyget har varit i drift en tid då det upptäcks att det har en sårbarhet som kan leda till att riktigheten i informationen inte kan garanteras.

Diskussionsfrågor:

3.1. Vilka risker ser ni på kort respektive långsikt?

3.2. Hur väljer ni att hantera dessa risker?

3.3. För att kunna hantera riskerna – vilken typ av frågor/uppdrag ställer ni till ansvarig i er organisation?

3.4. Vem/vilka i er organisation är ansvarig/a?

Understödjande frågor

Frågorna kan användas av diskussionsledaren i samband med gruppernas redovisning (anpassa efter gruppens mognad och hur diskussionen utvecklas):

- Vilka utmaningar såg ni?
- Hur resonerade ni kring förtroenderiskerna?
- Vilken roll har det främsta mandatet att agera?
- Hur kommunicerar ni kring den lösning ni valt?
- Har det skett någon förändring från förra momentet? Påverkas situationen av det som hände nu, och i så fall hur?

Sammanfattande diskussion

Tidsförhållanden

Total tid för momentet: ca 15 min.

Aktörer

Gemensam diskussion med samtliga deltagare.

Diskussionsfrågor

Vad tar ni med er från dagens diskussion avseende:

- Hur ledningen påverkar arbetet, kortsiktigt och långsiktigt.
- Utmaningar med att skapa och upprätthålla en säkerhetskultur.
- Informationssäkerhetsaspekter (riskanalyser) som en del av frågor inom andra områden, både i det dagliga arbetet och vid händelser.
- Informationssäkerhetsrisker i förhållande till andra risker och mål.

Diskussionsledaren avrundar och berättar om hur erfarenhetshanteringen kommer att gå till. Varje deltagare får svara på utvärderingsfrågorna innan passet avslutas.

Myndigheten för
samhällsskydd
och beredskap

651 81 Karlstad Tel 0771-240 240 **www.msb.se**
Publikationsnummer MSB2228 – reviderad oktober 2024 ISBN 978-91-7927-552-5