TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret

HUOLTOVARMUUSKESKUS
FÖRSÖRJNINGSBEREDSKAPSCENTRALEN
NATIONAL EMERGENCY SUPPLY AGENCY

Anvisning om cyberövningar

Handbok för övnings-arrangörer

Traficoms publikation
227/2020

Innehåll

Anvisning om cyberövningar
– Handbok för övnings-arrangörer
ISBN 978-952-311-716-7
ISSN 2669-8757
227/2020

1 Inledning

Denna övningsanvisning har upprättats av Cybersäkerhetscentret vid Transport- och kommunikationsverket i samarbete med Försörjningsberedskapscentralen. Anvisningen förutsätter ingen tidigare erfarenhet av cyberövningar. Den riktar sig till ansvariga för organisationers informationssäkerhet och it-förvaltning vars uppgifter inbegriper ansvar för organisationens cybersäkerhet.

I samband med Försörjningsberedskapscentralens program KYBER 2020 konstaterade man att det behövs en anvisning om cyberövningar i Finland. Det finns massor med information om olika övningssätt på nätet. Vi ville på ett praktiskt sätt sammanställa information om hur man ordnar övningar.

I denna anvisning berättar vi vad en cyberövning innebär, hur den ordnas och hur man genom regelbundna övningar kan dra största möjliga nytta för organisationens eget beredskapsarbete.

Vår anvisning innehåller bakgrundsinformation om vikten av övningar, praktiska råd om hur en övning arrangeras och en kort ordlista för cyberövningar. Dessutom ger vi anvisningar om hur övningsverksamheten kan integreras i organisationens årsplanering.

Vi hoppas att den ram som vår anvisning skapar inte begränsar utan fungerar som ett stöd i och en motor för er cyberövning när det är dags att gå från teori till praktik.

Försörjningsberedskapskritiska organisationer kan få enskilt stöd och hjälp i sin cyberövningsverksamhet av Cybersäkerhetscentrets stödtjänster för övningsverksamhet. Kontaktuppgifter till stödtjänsterna finns i slutet av denna anvisning.

Med hjälp av cyberövningsanvisningen kan en organisation

1. få anvisningar och råd i samband med en övning
2. starta upp sin egen cyberövningsverksamhet
3. planera sin första egna övning
4. förbättra sitt befintliga övningsprogram
5. förbättra sin beredskap för informationssäkerhetsincidenter och -störningar och förmåga att återhämta sig från dessa.

2 Vad är en cyberövning?

En cyberövning är ett övningstillfälle där en organisation modellerar och testar sin beredskap för olika cyberstörningssituationer. En övning innebär att en fiktiv situation som riktar sig mot organisationen målas upp på det sätt som bäst lämpar sig för ändamålet.

Cyberstörningssituationer är incidenter i organisationens informationstekniska verksamhetsmiljö som får konsekvenser för organisationens verksamhet. Med hjälp av en cyberövning simulerar, dvs. modellerar, man en cyberstörningssituation. På detta sätt skapas fiktiva omständigheter där man kan testa vilka konsekvenser en störning får och hur man återhämtar sig från dessa.

Man kan föreställa sig övningen som en gratis kris riktad mot organisationen där man själv kan välja tidpunkt och konsekvenser. Man kan få många värdefulla lärdomar av en krissituation och med hjälp av en övning kan man tillämpa denna inlärningsform utan att krisen stör organisationens verksamhet. En övning är ofta ett förmånligt sätt att hitta brister i krisberedskapen.

Många organisationer har sedan länge ordnat olika slags övningar. Till exempel ordnas räddnings- och utrymningsövningar i många lokaler för att upprätthålla brandsäkerheten. Livsviktiga kunskaper har också övats och lärts ut inom organisationernas första hjälpen-utbildningar.

Till skillnad från övningar i den fysiska världen är en cyberövning riktad mot organisationens cybermiljö. Det innebär att konsekvenser av störningssituationer i en till stor del uppkopplad verksamhetsmiljö bedöms mer långtgående än enskilda it-system. Det är alltså inte fråga om enbart en övning av funktionsstörningar i datorer. En cyberövning är inte enbart en it-övning.

Typiskt för cyberstörningssituationer är att de även får konsekvenser på annat håll än i den egentliga verksamhetsmiljön, bland annat i form av produktions- eller logistikstörningar. I en cyberövning kan man till exempel simulera en störning i logistikcentralens it-system som får konsekvenser för leverans och mottagning av varor.

I bästa fall blir omfattande konsekvenser av informationstekniska störningar klara för alla parter med cyberövningens hjälp och organisationens beroende av fungerande it-system tydligare. Övningen kan även uppdaga organisationens dolda beroendeförhållanden. Sådan kunskap skulle vara utmärkt för organisationens riskhanteringsarbete och för en mångsidig beredskap.

Utöver handlingssätt i undantagssituationer framhävs även kommunikation och ledning i övningarna. Många gånger kan man även samordna organisationens olika funktioner på ett verklighetstroget sätt varvid uppfattningen om hur olika helheter samarbetar förbättras. I de sociala mediernas tidsålder är i synnerhet kommunikationen i hanteringen av cyberstörningssituationer av central betydelse.

Man kan själv ordna en cyberövning eller låta en tredje part ordna den. Omfattande samarbetsövningar där representanter för olika organisationer deltar är ett bra tillfälle att utveckla samarbetsnätverk och skapa kontakter mellan olika organisationer. Olika samarbets- eller utbildningsorganisationer såsom läroanstalter eller statliga organisationer ansvarar för att producera omfattande övningar. Nyttan av att delta i omfattande samövningar är mycket stor.

Kontinuerlig och regelbunden cyberövning är en central del i en modern organisations cybersäkerhetshantering. Om er organisation ännu inte håller övningar, kan ni komma i gång med hjälp av denna handbok.

2.1 Varför ordna en cyberövning?

En övning lönar sig inte enbart för själva övningens skull. Om en övning har planerats och genomförts med utgångspunkt i organisationens behov och lärdomarna implementerats som arbetssätt, kommer organisationen med säkerhet att utvecklas.

Fungerar era processer för störningssituationer? En övning är ett utmärkt sätt för en organisation att säkerställa att de överenskomna handlingssätten i undantagssituationer är bra, effektiva och ändamålsenliga. I en övning kan man aktivt tillämpa de överenskomna sätten istället för att passivt granska dem. En övning kan även fungera som ett test av förnyade processer där man mäter hur de fungerar i verkligheten.

En cyberövning avslöjar styrkor och svagheter. I synnerhet att regelbundet ha tillämpat och återkallat krisanvisningar i minnet är till hjälp i en verklig situation. I några övningar har man inte ens kommit ihåg anvisningen för hantering av incidenter fastän det fanns en sådan!

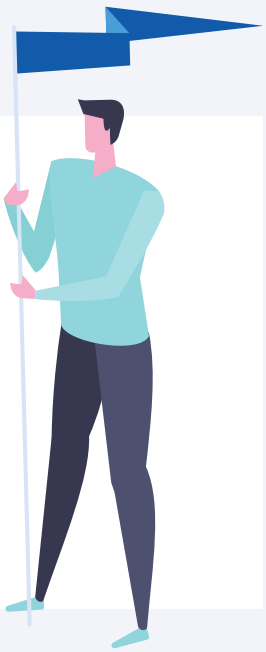
I många organisationer skjuter man hela tiden upp att inleda ett eget övningsprogram. Detta är förståeligt eftersom övningsverksamhet kan upplevas som något krävande och svårt som endast hör hemma i större organisationer. Det går emellertid att på kort tid inleda övningsverksamheten med i princip två tomma händer och utan större tid och ansträngning.

Ett fungerande och balanserat övningsprogram kan innehålla små övningar som är enkla att ordna och mer komplicerade operativa övningar. Också enkla skrivbordsövningar är nyttiga.

Den första övningen kan ordnas som en enkel skrivbordsövning. Detta ger ofta mersmak och därifrån kan resan mot mer mångsidiga, utmanande och intressanta övningar börja.

Fördelar med en övning

- organisationens kristålighet blir bättre
- ökad förståelse för it-systemens interna beroendeförhållanden
- ökad förståelse för omfattande konsekvenser av störningssituationer
- utveckling av den interna och externa kommunikationen
- ökad ledningsförmåga i undantagssituationer
- interna processer utvecklas genom analys av övningsresultaten
- ökat samförstånd mellan tjänsteproducenter och kunder
- ansvarsområden förtydligas
- förtroendet för att man kan hantera osäkerheter växer.



3 Olika typer av övningar

Det finns oändligt många olika typer av cyberövningar. När man planerar en egen övning är det bra att komma ihåg att den kan genomföras på många olika sätt. I själva verket kan vilken kontrollerad granskning som helst av processer fungera som en övning. De olika övningstyperna definieras av omfattningen av simuleringen av händelser, övningsmiljön, tekniska krav och tidsanvändning. Man kan välja ut element från många olika typer till sin egen övning enligt behov.

Valet av lämplig övning beror på tillgängliga resurser, målet med övningen och målgrupp. En övning som ordnas för teknisk personal skiljer sig från en krishanteringsövning för ledningen både till genomförandesätt som målsättning. Det är bra att först fastställa mål och välja deltagare och först därefter övningsmetod.

Ledningens krisberedskap och den tekniska personalens kompetens kan inte utvecklas genom samma slags övningar. Övningstypen ska väljas utifrån vad man vill öva. Till exempel är skrivbordsövningar eller operativa övningar lämpliga för ledningsövningar. Däremot kräver en tekniskt kunnig övningsgrupp en mer tekniskt utmanande övningstyp. Genom att kombinera övningstyperna kan man ordna en ledningsövning och en teknisk övning samtidigt. Det är inte helt problemfritt att kombinera målsättningarna, vilket återspeglas i en mer komplicerad planering av övningen.

3.1 Skrivbordsövning

Lämpar sig för hantering och ledning av cyberstörningssituationer samt genomgång och utvärdering av processer för dessa situationer.

Övningar som till sitt genomförande är enklare och mer allmänna är så kallade skrivbordsövningar där man endast använder skriftligt material. I en skrivbordsövning modellerar man ingen händelsemiljö. I allmänhet får deltagarna ta del av övningshändelserna och uppgifterna i anslutning till dem i början av övningen.

Målet med övningen är att hitta och dokumentera lösningar och svar på de incidenter och uppgifter som skapats. Det är enkelt att förbereda övningen och det krävs inga långa förberedelser. I fråga om arrangemangen räcker det att deltagarna sammankallas vid en på förhand avtalad tid och plats för att lösa uppgifterna i spelet.

En skrivbordsövning innehåller vanligen ingen tidsinställd input eller någon interaktivitet, utan övningsuppgifterna utförs i lugn och ro. Man kan göra upp ett tidsschema för en övning som består av flera övningsuppgifter till exempel så att den första timmen funderar man på situation 1 och den andra timmen situation 2. Vanligen är slutresultatet ett skriftligt svar på frågor och en separat lista över saker man ska ta reda på i efterhand.

Uppgiften i en skrivbordsövning kan bestå av till exempel en fiktiv beskrivning av nuläget och en uppgift i anslutning till det, oftast i form av en fråga till exempel på följande sätt:

> ”En viktig leverantör och tjänsteproducent meddelar att hela affärsverksamheten har sålts till land X. Kommer försäljningen att inverka på bedömningen av tillförlitligheten hos tjänsterna?”

I en sådan övning är det centrala inte att utreda orsaken bakom störningen eller fördjupa sig i tekniska detaljer, utan att upprätta planer för undantagssituationer eller kontrollera huruvida befintliga planer är användbara och aktuella.

En skrivbordsövning kan även kallas ”pappersövning” eftersom den inte behöver ordnas i en teknisk miljö. Innehållet i spelet kan göras upp på förhand och skrivas ut till pappers som levereras till spellokalerna. När spelet börjar tar man fram beskrivningen av spelsituationen och övningen kan börja. Naturligtvis kan man även använda en teknisk miljö eller lämpligt verktyg för att ordna en skrivbordsövning.

Skrivbordsövningar fungerar bra även som en ”uppvärmning” inför mer intensiva övningar. Då kommer deltagarna i lämplig stämning eller får möjlighet att repetera kunskaper och färdigheter som behövs i den kommande övningen.

3.2 Grundorsaksanalys (pre-mortem)

Lämpar sig för att förutse problem och styra riskhanteringen.

Grundorsaksanalys, även kallad pre-mortem, är en övningstyp som genomförs på samma sätt som en skrivbordsövning. Övningen är operativt enkel och lätt att ordna. Målet med denna analys är att hitta riskernas grundläggande orsaker som leder till cyberstörningssituationen när de blir verklighet.

En förverkligad cyberstörningssituation läggs fram för deltagarna och deras uppgift är att fundera över vilka faktorer i deras verksamhetsmiljö som skulle kunna förorsaka ett slutresultat i likhet med detta. Övningen spelas som om man börjar från mitten och bedömer händelsernas startpunkt.

Identifierade risker kan användas som grund för scenarioarbetet för kommande övningar. Till exempel kan en dataläcka där kunddata har blivit offentliga användas som en förverkligad risk i en grundorsaksanalys. Deltagarnas uppgift är att utarbeta olika kränkningar av informationssäkerheten till följd av vilka dataläckan har kunnat uppstå i detta fall.

3.3 Operativ övning

Lämpar sig för krisledning, övning av kriskommunikation och samarbetsövningar.

En operativ övning är en mer realistisk metod än en skrivbordsövning. Bland annat är tidspressen betydligt stramare eftersom man hanterar tidsplanerade input i övningen. De serveras deltagarna utifrån ett på förhand upprättat manus som för handlingen i övningen framåt.

Input i övningen är enskilda meddelanden som beskriver händelser i övningen. Input kan vara vilken informationshelhet som helst som för spelet framåt, till exempel:

- ett e-postmeddelande
- ett telefonsamtal
- en tweet
- en nyhet
- ett Facebook-inlägg
- information som deltagarna får per telefon från spelcentralen
- en begäran om en intervju.

Denna övningstyp framhäver övningsdeltagarnas förmåga att leva sig in i situationen, kommunicera sinsemellan och skapa en aktuell lägesbild över hur händelserna i övningen påverkar organisationen.

I en bra övning får deltagarna lite information om händelserna åt gången och spelet består av flera händelser från många olika håll. Till exempel utmaningar i anslutning till sociala medier och kommunikation är enkla att införliva i spelet genom nyheter och meddelanden på sociala medier som kommenterar spelhändelserna. Även begäran om intervjuer från medier och ”riktiga” intervjuer med videoinspelningar ger möjlighet att öva extern kommunikation i svåra situationer. Samtidigt ökar de övningens svårighetsgrad.

En effektiv och dynamisk spelcentral är en viktig del av en operativ övning. Spelcentralen är ett avskilt utrymme från deltagarna där spelets planerare styr spelet. Centralens uppgift är att leda spelet och skicka input till deltagarna under spelets gång. Utöver huvudinput som planerats på förhand kan centralen skicka betingade input till spelet för att reagera på deltagarnas lösningar och beslut. Ny input kan även behövas i en situation där deltagarna styr spelet i en oförutsedd riktning.

Som hjälp i planeringen kan man använda en övningssimulator som samlar ihop input på ett ställe där deltagarna kan ta fram och granska dem. Mer information om övningssimulatorer finns i kapitel 6.7 Modellering av övningsmiljön.

3.4 Teknisk övning

Lämpar sig för höjning av tekniska färdigheter, introduktion till system och återställningstester.

En teknisk övning kräver stora förberedelser. Tanken är att övningsupplevelsen sker direkt i den informationstekniska miljön där man skapar en undantagssituation, och övningen består av att identifiera, utreda, avhjälpa och dokumentera denna.

I en teknisk övning kan man mycket realistiskt simulera olika störnings-, fel- och hotsituationer. Övningen kan även grunda sig på att testa ibruktagande av reservsystem, att återställa säkerhetskopior eller något annat som säkerställer produktionssystemens funktion i undantagssituationer.

Övningens innehåll kan till exempel vara att en okänd enhet som är ansluten till organisationens nät skickar trafik till en dator utanför organisationen som kontrolleras av ”angriparen”. Till produktionsnätet ansluts för övningen en enhet som simulerar en skadlig enhet som producerar extraordinär trafik. Övningen inleds genom att deltagarna får information om den första observationen utifrån vilken de måste vidta rätt åtgärder för att lösa problemet.

Övningsmiljön har en viktig roll eftersom man med denna övningstyp kan komma mycket nära verkliga handlingsmodeller och processer. Det krävs självfallet stora resurser för att skapa eller beställa olika program som simulerar enheter eller skadliga program. En teknisk övning rekommenderas i organisationer som redan har granskat hanteringen av undantagssituationer med hjälp av andra övningssätt och säkerställt att processerna i anslutning till detta fungerar och är uppdaterade.

En teknisk övning kan även genomföras i en helt simulerad miljö. I simulerade miljöer skapas ett nätverk, arbetsstationer och tjänster för övningsdeltagarna. Incidenterna som uppkommer i dessa undersöks med verktyg som är allmänt tillgängliga eller i allmänt bruk. Bland annat kan avsaknaden av egna verktyg samt skillnaderna mellan övningsmiljön och produktionsmiljön påverka övningsupplevelsen även om övningen är sanningsenlig. Det krävs även att deltagarna har förmåga att anpassa sig till situationen och följa organisationens processer även i en främmande informationsteknisk miljö.

3.5 Capture the flag-övning

Lämpar sig för utveckling av tekniskt kunnande och för att bekanta sig med system.

Målet med Capture The Flag, dvs. CTF-övningar är att hitta ”flaggor” i informationstekniska system som ger deltagaren eller -laget poäng. Flaggorna kan till exempel vara ett visst slags tecken- och bokstavsrader som deltagaren matar in i poängsystemet när de hittas. I CTF-övningar kan flaggorna vara gömda på många olika platser, men vanligen ska deltagarna ta sig in i ett skyddat system och göra olika utredningar i systemet varvid flaggorna uppenbaras.

CTF-övningar är tekniska övningar där merparten är en tävling mellan olika deltagare eller lag. CTF-övningar ordnas i samband med olika slags tillställningar eller utbildningar samt som öppna tillställningar via internet.

På internet finns det olika fritt tillgängliga virtuella miljöer som har skapats för att genomföra tekniska övningar. Det är möjligt att utnyttja dessa när man ordnar en egen CTF-övning. Man kan hitta fritt tillgängliga CTF-övningar på nätet till exempel genom att söka på ”CTF challenge” eller ”capture the flag cyber exercise”.

CTF är ett enkelt sätt att börja en teknisk övning. En organisation kan samla ihop ett eget lag och delta i en CTF-tävling eller -tillställning. Någon annan har ansvaret för att ordna övningen, men den tekniska personalen får bra övning i att undersöka och utreda sårbarheter även i de egna nätverken.

Allmänt tillgängliga virtuella CTF-miljöer eller -övningsplattformar är dåligt lämpade för granskning av en organisations egna processer, men de fungerar bra när man vill öka den egna tekniska personalens kunnande.

3.6 Stora samövningar

Lämpar sig för att skapa nätverk, stärka samarbetet och skapa en lägesbild.

I Finland har man redan länge ordnat flera stora samövningar, allt från tekniska övningar mellan myndigheter till att skapa interaktionsnätverk mellan organisationer. I dessa övningar följer man huvudsakligen reglerna för en operativ övning i kombination med drag ur skrivbordsövningar. Även en simulerad internetmiljö har använts. På detta sätt har övningen fått samma innehåll som en teknisk övning.

Istället för att förbättra egna interna processer är målen för en samövning att granska organisationens nätverk och värdekedjor. I samövningar fokuserar man på att skapa en gemensam lägesbild samt att samordna den egna organisationens och samarbetsparternas verksamhet. Ofta vill man dessutom öva informationsutbyte och att skapa en allmän uppfattning om angriparens motiv, tillvägagångssätt och mål.

Vissa samövningar fokuserar på ett tekniskt spel där de deltagande lagen tävlar mot varandra genom att försvara sin egen spelmiljö och samla poäng.

I allmänhet krävs det inte att en organisation har tidigare övningserfarenhet för att delta i en samövning. I början av övningen ordnas ett informationstillfälle där man går igenom övningens mål, deltagare och praktiska aspekter. Det är ofta mycket arbete med att ordna en samövning, men deltagandet kräver endast sällan stora satsningar av organisationen jämfört med nyttan av övningen.

Samövningar kräver i regel inbjudan. Om er organisation får möjlighet att delta i en samövning lönar det sig att utnyttja den eftersom samövningar är utmärkta sätt att bekanta sig också med andra övningsmetoder.

Före övningen lönar det sig för organisationen att fastställa sina egna målsättningar och förbereda sig så långt möjligt. Då får man ut största möjliga nytta av samövningen. Det är i synnerhet skäl att noga fundera igenom vilka roller och ansvar personer som deltar i övningen har och se till att rollerna motsvarar verklighetens behov.

4 Förberedelser inför en övning

Övningens livscykel kan beskrivas genom tre skeden: förberedelse, genomförande och efteranalys. I synnerhet efteranalys och implementering av lärdomar i organisationens verksamhet är centrala för nyttan av en övning. En noggrann planering säkerställer vidare att man noga har funderat på övningens förlopp och detaljerna. Förberedelse och efteranalys är största delen av övningshelheten, men samtidigt är de en förberedelse inför nästa övning. Förberedelse, genomförande och efteranalys utgör även ett kontinuum – övningens kretslopp.

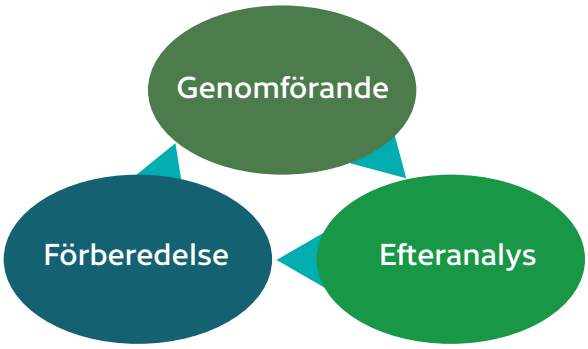
Den övningstyp som har valts påverkar hur arbetsdryga förberedelserna är. Förberedelsen inför en skrivbordsövning eller en grundorsaksanalys är enklare än inför en operativ övning, men det är skäl att avsätta tillräckliga resurser för analys av resultaten.

Många gånger kan det vara motiverat att ordna flera enkla övningar per år med en snäv tidtabell än att lägga mycket tid och energi på en stor övning per år.

Förberedelserna är det mest arbetsdryga skedet av en övning. Även om man köper en övning som en tjänst, måste alla reservera tillräckligt med tid för planeringsmötena. Det är bra att boka in övningens planeringsmöten i god tid, minst tre månader före den egentliga övningen.

De som utsetts att planera övningen ska redan i ett tidigt skede engageras att förbereda övningen. Planeringen sker under arbetstid, vilket ska beaktas i hur personernas övriga uppgifter ordnas. Om planerarna är frånvarande från planeringsmöten stör det genomförandet av hela övningen eftersom de ska ha kontroll över övningen som helhet.

Allt kan inte planeras på förhand, men det är bra att fastställa övningens ramar så exakt att utrymmet för överraskningar bli så litet som möjligt. Att anlita en utomstående arrangör är ofta en bra lösning eftersom planeringsarbetet slukar en stor del av organisationens egna anställdas arbetstid.



Planeringen liknar ett litet projekt. Om man själv har hand om planeringen, kan man tillämpa följande exempelstruktur i arbetet:

Brainstorming om övningen
- preliminära utredningar
  - övningens mål
  - övningens omfattning
  - föremål för övningen
  - möjliga tidpunkter för övningen
- preliminär tidtabell för planeringsarbetet
- ansvarsfördelning.

Planeringsmöte 1:
- projektet inleds
- en projektarbetsgrupp utses
- resurser för projektet anslås
- målet för övningen bestäms
- val av övningsmetod.

Planeringsmöte 2:
- utkast till övningens innehåll
- dokumentation för övningen upprättas
- deltagare väljs ut och bjuds in
- lokaler bokas.

Planeringsmöte 3:
- bearbetning av övningens innehåll eller input
- dokumentationen ses över och färdigställs
- deltagarna bekräftas.

Genomförande
- förberedelse
- övning
- omedelbar respons (Hot wash-up)

Åtgärder efter övningen
- observatörernas rapportering färdigställs
- deltagargrupperna går igenom vad de lärt sig
- uppföljning av hur lärdomar omsätts i praktiken.

Projektet avslutas och utvärdering av helheten

En ny övning planeras enligt årsklockan

En fördel med att ordna övningen själv är mindre kostnader och möjligheten att ordna övningar flexibelt i egen takt. Man kan även köpa in en stor del av arbetet med att planera och förbereda övningen av en utomstående leverantör. Då sparar man sin egen tid, i synnerhet om man har anlitat en erfaren och yrkeskunnig person. Emellertid kräver detta en stor insats av beställaren, eftersom övningen måste planeras i enlighet med organisationens mål och verksamhetsmiljö. Man kan inte köpa en personlig ”nyckelfärdig” övning.

Under planeringen uppstår mycket skriftligt material som ska upprättas och sparas så att det lätt kan hittas och användas också i fortsättningen. Till exempel kan övningens responsenkät, olika blankettmallar eller allmänna instruktioner till deltagarna användas på nytt utan större förändringar.

4.1 Fastställande av målet

Övningens förlopp från planeringsskede till efteranalys styrs av ett huvudsakligt mål som man bör fastställa genast i början av processen. Det kan hänföra sig till effektivisering av verksamheten, säkerhet, kompetensutveckling eller testning av någon process. Det huvudsakliga målet härleds från organisationens strategi och riskhanteringsarbete.

Målen bör beskriva verkliga och befintliga behov. Om övningsverksamheten fortsätter hela året, kan årsspecifika huvudmål delas upp i underordnade mål och egna övningar ordnas för vart och ett av dessa.

Det huvudsakliga målet kan till exempel vara ”cyberkrishantering enligt processen Major Incident Management”. Som underordnade mål kan man fastställa ”tillämpning av anvisningar om kriskommunikation”, ”test av övergång till reservsystem” och ”fastställande av aktuella kontaktuppgifter”. Utifrån målen kan man börja planera till exempel en operativ övning där man simulerar en

kris som omfattar kommunikationsbehov samt kontakt till tjänsteproducenter.

Om målet är tillräckligt konkret kan man i efterhand konstatera huruvida det uppnåddes eller inte. I fråga om målsättningar av typen process x ska förbättras" är det svårt att konstatera eller se huruvida man har lyckats eller misslyckats.

Övningens mål kan till exempel hänföra sig till:

- utveckling av krisledning eller -kommunikation
- förbättring av teknisk beredskap
- återhämtning från störningar
- observation av hot
- rapportering
- test av kontaktmetoder och reservmetoder
- test av processer för att hantera störningar
- test av tekniska system, samarbete med leverantörer och tjänsteproducenter eller förtydligande av ansvarsfördelningen.

Det lönar sig att upprepa målen vid varje planeringsmöte inför övningen så att man tydligt har dem i åtanke. De ska även klargöras för deltagarna så att alla parter har ett gemensamt mål.

4.2 Faktorer som påverkar valet av övningstyp

Vilken tillställning som helst där organisationens verksamhet testas och utvecklas kan genomföras som en övning. Det är bra att ha denna princip i åtanke när man väljer övningstyp efter att man först har fattat beslut om övningens mål, omfattning och deltagare.

Övningstyperna begränsar inte planeringen av övningen, utan det är fritt fram att kombinera lämpliga drag och egenskaper från olika typer. Till exempel kan man lägga till drag från en skrivbordsövning och en teknisk övning till en operativ övning.

Det lönar sig att anlita utomstående hjälp när man planerar en komplicerad övning. En kommersiell och erfaren aktör fokuserar på det väsentliga och kan även hjälpa till att starta upp en organisations egen övningsverksamhet.

En övning kräver inte nödvändigtvis alltid fysisk närvaro. En övning kan även spelas så att deltagarna inte sitter på samma ställe för att diskutera frågor. I synnerhet i organisationer som verkar inom ett stort geografiskt område kan distansförbindelse minska behovet av resor. Under övningen kan vissa ha konsultativa roller och vara tillgängliga vid behov och delta i spelet en kort stund per telefon eller annan distansförbindelse. Till exempel kan det ibland behövas juridisk hjälp.

Distansförbindelse och att delta i en övning parallellt med det egna arbetet kan emellertid påverka koncentrationen negativt. Därför bör personer som deltar på distans reservera tillräckligt med störningsfri övningstid i sin kalender.

Om man vill öva med en stor grupp åt gången, kan man för varje avskild lokal boka egna utrymmen för distansdeltagande. Man kan bland annat använda videokonferens, direktmeddelanden, mobiltelefoner eller e-post för distansdeltagande. Att använda distansförbindelse är ett bra sätt att testa organisationens kommunikationskanaler och vid behov reservförbindelser om situationen i övning förhindrar användning av de primära kontaktmedlen.

5 Planering av en övning

När en övning genomförs står organisationens ledning, planerarna, deltagarna och personer i stöduppgifter i en central ställning. Ju större övning det är frågan om, desto fler människor behövs i olika roller.

Ledningen ska vara tydlig med sitt engagemang och intresse för övningen och lärdomarna av den. Planeringsarbetet blir lidande om inte ledningen tydligt stöder övningen eftersom deltagarna kan uppleva att deras arbetstid används för onödiga saker.

Om man i övningen kan testa organisationens verksamhets kontinuitet i undantagssituationer och kan konstatera att funktionsförmågan är intakt, gagnar denna information även organisationens ledning.

Härnäst följer en beskrivning av centrala uppgifter och arrangemang i fråga om planering och genomförande av en övning.

5.1 Att sätta ihop en planeringsgrupp

Det är bra att boka in åtminstone tre eller fyra planeringsmöten. Dessutom krävs det särskild planeringstid för att skapa övningens berättelse och input. Personer som ingår i planeringsgruppen bör inte vara deltagare i övningen eftersom deras förkunskaper om vad som kommer att hända i spelet åtminstone skulle påverka spelets förlopp. Planeringsgruppen kan även kallas för en projektgrupp.

Planeringsgruppen måste ha en ledare som sammankallar gruppen och ansvarar för att leda övningen. Ledaren är även projektchef för övningen. I gruppen ska det även finnas sakkunniga från organisationen som ansvarar för övningens innehåll och som är väl insatta i organisationens verksamhet. För att få nya perspektiv och kunskaper kan man även bjuda in utomstående sakkunniga, tjänsteproducenter eller representanter för andra samarbetspartners till gruppen.

Var och en i planeringsgruppen måste känna till sin roll och sina uppgifter. När man samarbetar med en utomstående övningspartner ansvarar partnern i allmänhet för att leda planeringsarbetet, att ordna planeringsgruppens möten och fördela rollerna mellan planerarna enligt deras styrkor.

Exempel på representation och roller i planeringsgruppen:

- övningsledare: it-säkerhetschef eller -direktör eller utomstående partner
- ledare för scenarioplaneringsarbetet: it-säkerhetssakkunnig eller utomstående partner
- övningens interna och externa kommunikation: kommunikationssakkunnig eller -chef
- it-förvaltning, it-system och utomstående leverantörer
- affärsverksamhetsenheternas representant: key account manager eller motsvarande
- tjänsteproducent: samarbetsföretagets representant
- tjänsteproducent: it-säkerhetstjänsternas representant

Med en sådan sammansättning kan man mycket bra ta reda på vilken slags övning som kunde gagna organisationen bäst och hur den bör förberedas. Gruppen ovan är bara ett exempel som kan användas som ett stöd för den egna planeringen.

5.2 Val av deltagare

Om målet med övningen är att förbättra ledningen i en krissituation, behöver åtminstone organisationens ledning och kommunikation utgöra deltagare i övningen. Om målet däremot är att förbättra produktionssystemets funktion i en undantagssituation, väljs personer som arbetar med produktionssystemet ut som deltagare. Rätt deltagargrupp i en informationsteknisk övning är organisationens informationstekniska personal jämte chefer.

En övning kan innehålla uppgifter för vilka det behövs flera olika representanter för organisationens personal. Det rekommenderas att kommunikationen närvarar vid alla övningar eftersom den har en betydande roll i hanteringen av cyberstörningssituationer – i synnerhet i situationer där störningen får konsekvenser utanför organisationen. Även när man övar interna störningssituationer kan kommunikation vara till hjälp när man upprättar lämpliga meddelanden till organisationens personal och intressenter.

Deltagare med mindre roller kan sköta spelets stöduppgifter från sin arbetsstation parallellt med sina arbetsuppgifter. En deltagare behöver inte vara på plats under hela övningen om deltagarens roll består till exempel av att svara på några frågor. Oavsett om en deltagare har en stor eller liten roll, är det skäl att utse en suppleant för var och en som kan utföra den ursprungliga deltagarens uppgifter om denne är frånvarande. På detta sätt stannar övningen inte upp på grund av oförutsedd frånvaro.

Personer som är väsentliga i fråga om övningens innehåll är ofta med och planerar övningen. Vanligen är de inte själva med som deltagare i övningen. Istället för planerarna kan till exempel suppleanter delta i övningen eller så kan planerarna vara tillgängliga endast per telefon under övningens gång. I en sådan roll ska planeraren fokusera på att lösa problemen i övningen endast i ljuset av de fakta som deltagarna uppger. En medlem ur planeringsgruppen kan spela med i övningen men eftersom hen känner till övningens vändningar och överraskningar bör hens roll i spelet anpassas därefter.

Antalet roller i en övning är inte synonymt med kvalitet. Om för många deltagare bjuds in, kan själva övningssituationen bli kaotisk. Till exempel behöver den högre ledningen inte vara på plats vid en övning som ordnas för teknisk personal. Däremot är det viktigt att mellanledningen eller lagens chefer är närvarande i situationer som kräver beslutsfattande.

Deltagarnas roller i spelet hör i regel ihop med deras verkliga arbetsuppgifter.

Den som väljs ut till en övning ska ha tid att delta. Inklusive förberedelser och genomgång tar en övning vanligen en hel dag.

5.3 Förberedelser

För de flesta är en övningssituation en exceptionell händelse och därför är det inte nödvändigtvis självklart för deltagarna hur man förbereder sig inför en övning.

Deltagarna ska i god tid informeras om vilken utrustning eller vilka arbetsredskap de behöver ha med sig till övningen. Om deltagarna behöver egna datorer i övningen, ska detta göras klar och man ska även säkerställa att det finns tillräckliga nätförbindelser i övningslokalen. Ibland är det bättre utan den störning en dator innebär, eftersom e-post och direktmeddelanden lätt kapar deltagarens intresse. I övningsinbjudan ska det däremot tydligt anges vad deltagarna behöver ha med sig till övningen och vilken utrustning som inte får användas.

Det viktigaste är att ha ett öppet sinne och förhålla sig positivt till övningen samt agera i enlighet med händelserna under övningen. Deltagarna får ibland spela ”mot spelet” dvs. hitta kryphål i det för att kunna kringgå utmanande spelsituationer.

Ibland blir deltagarna för ivriga och ”spelar över” och gör drag som man inte ens skulle överväga i verkligheten på grund av stora kostnader. Till exempel: Systemet som används för att övervaka gränsöverskridningar fungerar dåligt och det finns misstanke om att det har hackats. Man löser problemet genom att stänga landets yttre gränser så att man inte längre behöver använda systemet.

I verkligheten skulle man självfallet inte lösa problemet på detta sätt. I övningen är det alltid skäl att sträva efter realism både vad gäller händelser och lösningar.

Spelcentralens uppgift är tygla under- och överspel. Centralen kan meddela deltagarna att den valda lösningen inte lyckas, varpå deltagarna måste komma på en annan lösning. Det är skäl att informera deltagarna före övningen om riskerna med över- och underspel så att de är medvetna om gränserna för sitt agerande samt de möjligheter som övningen erbjuder.

5.4 Stöduppgifter och observatörer

Man kan även knyta människor från andra organisationer eller enheter till övningen i jourhavande roller. De finns inte på övningsplatsen, men är redo att svara på deltagarnas frågor under övningens gång. I vanliga fall är personerna i dessa roller till exempel jurister som spelarna vid behov kan be om juridisk tolkningshjälp. Den jourhavande rollen passar även en leverantör eller tjänsteproducent om vars förmågor och svarstider det kan uppstå frågor under övningen.

Deltagarnas chefer och högre ledning kan också placeras i stödroller, såvida de inte är egentliga deltagare i övningen. Man kan även öva självständigt beslutsfattande och alternativa modeller för beslutsfattande genom att under pågående övning avlägsna dem som arbetar i stöduppgifterna.

Det lönar sig även att använda observatörer vid övningen. Dessa har en viktig roll i analysarbetet efter övningen. En observatör iakttar men ingriper inte i det spelarna gör. Observatören rapporterar också sina observationer till deltagarna och övningsarrangörerna efteråt. Observatören kan vara en person inifrån organisationen eller en utomstående.

Det centrala i uppgiften är att man inte ingriper i spelarnas handlingar eller beslut. I praktiken ska observatören inte diskutera med personer som deltar i spelet. Vid behov kan observatören förmedla information till spelcentralen om hur övningen framskrider och om eventuella problemsituationer under övningens gång. Man ska komma överens om detta på förhand.

Observatören antecknar sina observationer i en observatörspromemoria. Om det är möjligt kan man använda flera observatörer och fördela spelets olika delområden mellan dem. En kan fokusera på att bedöma beslutsfattandet och en annan övningsarrangemangen.

I efteranalysen av spelet ger observatörerna direkt respons till deltagarna och övningsarrangörerna. Senare lämnar de in sin renskrivna observatörspromemoria utifrån vilken framtida övningar kan utvecklas. Istället för en promemoria kan observatörerna även besvara den responsenkät som skickas ut efter övningen där respondenternas roller har specificerats.

För observatörens promemoria kan man upprätta en blankett där man antecknar alla delområden som ska observeras i form av frågor eller fält som ska fyllas i. På detta sätt kan man styra observationen. På blanketten kan man till exempel fråga:

- ”Hur fördelades ledningsansvaret för situationen?”
- ”Beaktades kommunikation i rätt tid och i tillräcklig utsträckning?”

Det går inte att göra en uttömmande och allmänt tillämplig blankett och det behövs inte heller. Varje blankett ska upprättas för en specifik situation där övningens mål, insatsområden och deltagargrupp beaktas. Om observatören använder samma blankettmall i motsvarande övningar är det möjligt att följa hur övningsverksamheten utvecklas.

5.5 Utrymmen

Välplanerade utrymmen är en stor del av en smidig övning. Övningens typ, placering och antalet deltagare avgör i stor utsträckning vilka slags lokaler som behövs. Ett lag som utför en helhet behöver alltid ett rum: ett rum ska reserveras för deltagarna och ett annat för en eventuell spelcentral. Till exempel behövs ingen spelcentral vid en skrivbordsövning då hela övningen mycket väl kan utföras i ett och samma utrymme.

Om det finns flera deltagargrupper som utför olika uppgifter, är det bra att placera dem i olika rum eller dela upp rummet med skärmar. Bra ventilation i förhandlingsrummet och tillräckliga utrymmen garanterar att en övningssession som räcker länge inte blir onödigt tung. Man ske se till att det finns anteckningsmaterial, blädderblock eller whiteboard och vid behov även förfriskningar i övningslokalerna.

Att samla deltagarna i ett och samma utrymme gör det lättare för dem att koncentrera sig på övningen. Stämningen i en övningssituation känns ofta konstgjord jämfört med en verklig krissituation. I verkligheten skulle krisen i en typisk övningssituation vara i många dagar, men i övningen kan den förkortas till några timmar.

Övningslokalerna ska tydligt märkas ut till exempel med texten ”ÖVNING PÅGÅR” och datum. Även korridorer och övriga områden i närheten av utrymmet där deltagarna rör sig ska omsorgsfullt märkas ut för att undvika missförstånd. En eltagare kan diskutera sådant som rör övningen i telefon i korridoren och därmed oroa förbipasserande som hör en del av samtalet. Exempel på vikten av övningshygien: En anställd som inte känner till övningen råkar höra en deltagares samtal om att en kemikaliecistern har vält i lagret. Situationen leder till ett verkligt brandlarm.

Deltagarna ska ha klart för sig var man får diskutera saker som gäller övningen. Det är särskilt viktigt att märka ut utrymmena om övningen omfattar en ledningscentral eller andra operativa utrymmen.

I operativa övningar kan man öppna en enkelriktad videoförbindelse från spelcentralen till deltagarnas utrymme. Via videolänken kan man övervaka deltagarna och styra spelet utifrån deltagarnas reaktioner. Video- och ljudförbindelsen kan genomföras till exempel så att man ringer ett videosamtal med en bärbar dator där videokameran på spelcentralens sida är övertäckt och mikrofonen är avstängd.

Under övningen hålls ofta en lunchpaus. Kring lunchen kan man bygga in ett ”tidshopp” i övningen, till exempel till följande dag. På detta sätt kan man föra spelet framåt utöver den till övningen begränsade tiden.

Om det är många som deltar i övningen, är det bra att reservera ett separat utrymme för lunchen. En diskussion i en allmän lunchrestaurang kan spridas från bord till bord och starta rykten.

6 Övningens innehåll

I vanliga fall är händelserna i övningen förlagda till nutid och nuvarande verksamhetsmiljö. I övningen följs organisationens befintliga strukturer och vardag. Vid behov kan man skapa fiktiva omständigheter där man till exempel övar i framtida eller exceptionella omständigheter. Utgångspunkten för en övning som är förlagd till framtiden kan till exempel vara verksamhet utomlands som i verkligheten ännu bara är under planering, men som i övningen redan har förverkligats.

Ibland kan en övning äga rum i en helt fiktiv miljö. Detta förfarande kan användas till exempel i stora samövningar där det är omöjligt att varje deltagare ska kunna följa sin verkliga arbetsbeskrivning. Målen för övningen kan då också anges på en högre nivå, till exempel utveckling av samarbetet inom nätverket.

6.1 Övningsscenario

Övningsscenariot är de fiktiva omständigheterna i övningen och händelsernas narrativ. I övningen grundar sig scenariot vanligen på ett it-säkerhetsproblem och dess bakgrund.

Organisationens eget riskhanteringsarbete ger bra vägledning för att bygga upp ett scenario. Utifrån identifierade risker kan man skapa scenarier som grundar sig på att riskerna blivit verklighet och lett till följande händelser. Alternativt kan man hålla ett kort möte där man brainstormar fritt om olika hot som kan tänkas röra organisationen. Det lönar sig också att använda nyheter inom teknologibranschen och Cybersäkerhetscentrets cyberväder när man bygger upp scenarier.

När man skapar ett scenario börjar man från en koncis beskrivning av problemet, dvs. man definierar scenariots kärna. Till exempel ”vårt lagerhanteringssystem är inte tillgängligt under 72 timmar.” Utifrån detta grundproblem bygger man upp ett övningsscenario dvs. de omständigheter som leder till att problemen uppstår, men även de konsekvenser som problemen får. Det är deltagarnas uppgift att lösa problemen. Det kan se ut på följande sätt:

”En av våra tidigare anställda har grälat med sin chef. Arbetstagaren har haft åtkomst till lagerhanteringssystemets centralserver där hen har lämnat ett skadeprogram som raderar serverns hårddisk vid midnatt den 1 mars. Händelserna i spelet är förlagda till morgonen den 2 mars.

De första arbetstagarna anländer till logistikcentralen men kan bland annat inte skriva ut försändelselistor eller kontrollera beställningar. Logistikcentralens verksamhet lamslås. Det blir stockning vid inkörsporten eftersom långtradarna som sköter transporterna inte får de produkter de behöver från vårt lager. Störningen påverkar även trafiken i närområdet.”

I en operativ övning informeras deltagarna inte genast om övningsscenariot, utan den första inputen upprättas baserat till exempel på det meddelande som personalen på morgonskiftet skickar till it-förvaltningen. Input skapas enligt scenariot och dess uppgift är att informera deltagarna om händelserna i scenariot under övningens gång.

I en skrivbordsövning kan scenariot beskrivas för deltagarna i början av övningen till exempel som i exemplet ovan. I denna övningstyp identifierar och löser deltagarna problem och problemsituationer som uppstår till följd av scenariot.

6.2 Input

Input är information enligt vilken man går framåt i spelet. Spelcentralen ger spelarna input via någon kommunikationskanal. Användningen av input och innehållet i dem varierar beroende på speltyp.

I praktiken är input ett informationspaket som ger deltagarna information om händelserna i spelet. Input kan vara:

- ett e-postmeddelande
- ett fotografi
- ett brev
- ett telefonsamtal
- en nyhetsartikel
- ett inlägg på sociala medier
- ett fysiskt föremål
- en fil eller ett dokument
- ett meddelande från en myndighet eller något annat som på något sätt beskriver händelserna i scenariot.

När man upprättar input kan man till exempel använda ett kalkylprogram som hjälp. Då kan man enkelt samla alla input i tidsordning. Tabellen kan användas för att följa med hur spelet framskrider. Det lönar sig att bygga upp input hierarkiskt så att input som hör till en och samma händelse samlas under samma rubrik. Detta förtydligar planeringen av övningen och gör det lättare att överblicka händelserna.

Exempel på hierarkin för
en inputtabell:

Händelse 1
Angrepp mot kunddatabas

- Händelse 1.1 – Dataintrång
  - Input 1.1.1 – E-postmeddelande
  - Input 1.1.2 – Telefonsamtal
  - Input 1.1.3 – Begäran om en intervju
- Händelse 1.2 – Utpressning
  - Input 1.2.1 – Myndighetsmeddelande
  - Input 1.2.2 – Brådskande begäran

Händelse 2
Kritisk haveri

- Händelse 2.1 – Produktionssystemet stannar
  - Input 2.1.1 – Telefonsamtal
  - Input 2.1.2 – E-postmeddelande
- Händelse 2.2 – Offentligt meddelande
  - Input 2.2.1 – E-postmeddelande

Inputinformation som samlats i tabellen kan innehålla bland annat följande:

- ordningsnummer
- publiceringstidpunkt
- händelse som inputen hänför sig till
- beskrivning av inputen
- mottagare
- avsändare
- typ av input (e-postmeddelande, telefonsamtal, brev, bild...)
- inputens innehåll (e-postmeddelande, samtalsmanuskript...)
- inputens status (spelat, väntar, förkastas)
- avhängighet till andra input.

Input förbereds så långt som möjligt på förhand så att de kan skickas till spelarna utan fördröjning. Spelcentralen följer inputtabellen under hela övningen och skickar inputmeddelandena vid den på förhand fastställda tidpunkten eller som reaktion på ett beslut eller en åtgärd som deltagarna vidtar. När input skapas

Kl.	Nr	Händelse	Beskrivning av inputen	Avsändare	Mottagare	Typ av inputen	Inputens innehåll	Status
9.00	1	Anvisningar för spelet	STARTEX	Spelcentralen	Alla övnings-deltagare	E-post	***ÖVNING***ÖVNING***ÖVNING*** Övningen har börjat. Input kommer att skickas från denna e-postadress. ***ÖVNING***ÖVNING***ÖVNING***	Spelat
9.30	2	Störning i registrators-kontoret	Skadligt program	Spel-centralen	ICT-tjänster	E-post	***ÖVNING***ÖVNING***ÖVNING*** From: jukkis@gmail To: atk-tuki@organisaatio.fi Subject: Registratorskontorets dator fastnat - hjälp! Hej! Vi verkar ha problem med en av våra datorer här vid registratorskontoret. Vi kan inte logga in och det finns en konstig bild på skärmen. Kan någon komma och titta på det här? Vi är här på Loimaa-kontoret. Ni kan kontakta mig på numret 044 xxx xxxx. Min jobb-e-post fungerar inte så jag skickar det här från min privata adress. Hälsningar, Jukka Järvinen Registratorskontoret ***ÖVNING***ÖVNING***ÖVNING***	Väntar

är det skäl att beakta att deltagarna kan lägga förvånansvärt mycket tid på att hantera en enskild input, och det är därför omöjligt att ge en exakt tidsuppskattning för hur länge en enskild input hanteras, men den uppskattade tiden för hanteringen av en input ska beaktas i planeringen av spelet. De åtgärder som deltagarna förväntas vidta kan räknas upp under inputen. Utifrån detta man kan bedöma hur mycket tid man ska lämna mellan olika input. Antalet input ska vara rimligt.

Deltagargruppen består ofta av sakkunniga eller ledare från olika branscher. Då kan man till exempel rikta en input till it-förvaltningen samtidigt som man riktar en annan till kommunikationen. Deltagare som hör till olika funktioner kan parallellt spela händelser där man behöver i synnerhet deras sakkunskap. I en välutförd planering hör input i spel som spelas parallellt ihop och styr deltagarna att samarbeta men även att sköta sina egna uppgifter.

Det är endast fantasin som sätter gränser när man skapar input. I en övning i krisledning kan en input vara till exempel kontakter med journalister. Man kan till och med skicka in en journalist med en fotograf bland deltagarna för att göra en intervju i realtid om händelserna i spelsituationen. Olika input ger möjlighet att öva många slags förmågor som krävs för att utreda en cyberstörning som leder till en krissituation.

6.3 Bakgrundsbeskrivningar

Om övningen utspelar sig i omständigheter som avviker från verkligheten, kan man som stöd för övningsscenariot skapa ett bakgrundsmaterial (s.k. ”state of the world”), dvs. extra information om den värld där övningen utspelar sig. I vanliga fall utspelar övningen sig i organisationens nuvarande och verkliga verksamhetsmiljö och då behöver ingen bakgrundsbeskrivning göras upp.

I bakgrundsbeskrivningar kan man använda till exempel nyheter om tillspetsade politiska, ekonomiska, miljömässiga eller sociala situationer som inte påverkar spelets innehåll direkt. På detta sätt kan man styra och begränsa alternativen för deltagarnas beslutsfattande och ge liv åt spelet. Deltagarna kan redan på förhand få ta del av bakgrundsinformationen för att skapa motivation och inlevelse.

Som en introduktion till övningen kan man till exempel ha en nyhetssändning som skapats på förhand som visas för deltagarna strax innan övningen börjar. Nyhetssändningen kan innehålla nyheter om antingen sådant som direkt rör organisationen som deltar i övningen eller bakgrundsinformation om omständigheterna.

6.4 Kommunikation om övningen

Central information om övningen lämnas till deltagarna samt till andra organisationer på förhand i form av förberedda meddelanden.

Ett allmänt meddelande om övningen upprättas och delas ut internt i organisationen. Meddelandet innehåller information om när och var övningen ordnas samt vem som bjudits in att delta. Inbjudan till övningen ska skickas i god tid. På så sätt får man bekräftelse på att de inbjudna deltagarna kommer att delta och bindande anmälan.

En eller två veckor före övningen skickas övningsinstruktioner till deltagarna om de praktiska arrangemangen, målen med övningen, deltagare samt tidtabellen för övningsdagen.

Efter övningen skickas ett tackmeddelande till deltagarna och ett sammandrag av övningen och insamlad respons. Det är också bra att göra upp ett kort meddelande till den deltagande organisationen om slutresultatet och insamlad respons. Det lönar sig även att skriva ett offentligt meddelande om övningen eftersom övningen stärker bilden av organisationen i offentligheten som en aktör som tar cyberstörningssituationer på allvar.

Kommunikation är särskilt viktig i operativa övningar där det centrala är kommunikationen mellan deltagarna och spelcentralen. Spelcentralen ska till sitt förfogande ha åtminstone en e-postlåda enkom för övningen samt ett telefonnummer som fungerar som spelcentralens ”växel”. Från växeln kan deltagarna be att få tala med vem som helst som de vill diskutera med. Spelcentralen ansvarar för att spela den begärda rollen i telefon eller konstatera att den efterfrågade personen inte är anträffbar.

För dem som spelar olika roller vid spelcentralen kan man utöver växeln reservera egna telefonnummer så att spelcentralens representanter kan diskutera med olika deltagare samtidigt.

Ett gemensamt nummer till de myndigheter som deltar i övningen kan ordnas så att man vid behov får tag på polisen, Cybersäkerhetscentret eller någon annan myndighet som stöder övningen vid behov. De telefonnummer och e-postadresser som används samlas i en telefonkatalog för spelet och skrivs ut till deltagarnas förfogande. Andra kontaktuppgifter får inte användas i övningen, därför samlas även kontaktuppgifter till personer som deltar i övningen i stöduppgifter eller via distansförbindelse i katalogen.

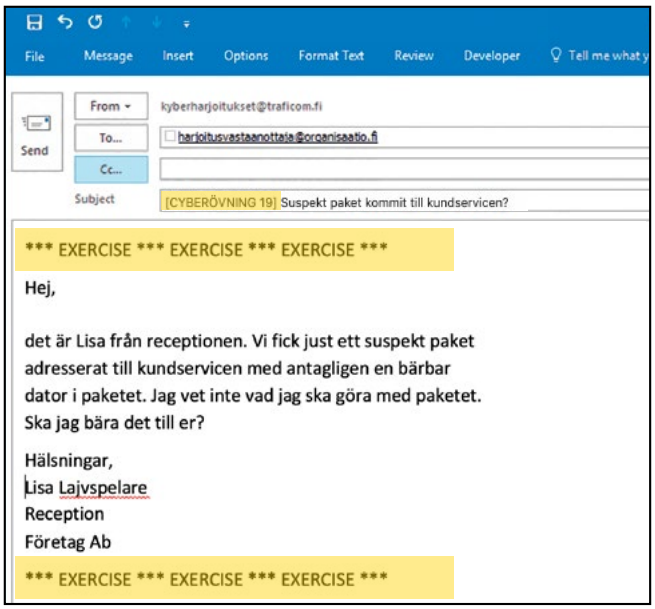
Spelcentralens e-postlåda ska följas hela tiden medan övningen pågår. Inkomna e-postmeddelanden ska läsas och besvaras konsekvent och utan dröjsmål. Om input förmedlas till deltagarna som e-postmeddelanden, kan den person vid spelcentralen som har hand om e-postlådan även vara den som skickar ut input.

6.5 Märkning av övningsmaterial

Meddelanden och dokument i anslutning till övningen ska märkas tydligt så man ser att de är övningsmaterial. Till exempel är det bra att i sidhuvudet och -foten i dokument skriva ÖVNING med röd text.

Det är också bra att under övningen hantera dokument som innehåller fiktiva personuppgifter i enlighet med lagstiftningen om dataskydd. Onödiga dokument ska förstöras efter övningen i enlighet med deras skyddsklassificering eftersom dokument som hör ihop med övningen även kan innehålla information som är känslig på riktigt.

Enligt gängse praxis kan e-postmeddelanden märkas ut på det sätt som visas i exemplet. Märkningar i anslutning till övningen är understrukna:



Övningens beteckning har angetts i meddelandets rubrik. På detta sätt kan man enkelt hitta och filtrera meddelanden som rör övningen.

Överst i meddelandefältet signalerar man tydligt att det är ett övningsmeddelande, till exempel genom att skriva ”exercise” eller övning”. Innehållsfältet avslutas också med en markering som anger att det är fråga om en övning.

På grund av övningshygienen är det viktigt att använda en tydlig märkning. Ett meddelande i anslutning till en övning som lösgjorts från sin kontext kan tolkas felaktigt. I övningsmeddelandets innehållsfält är det bra om det tydlig står vem som har skickat meddelandet, eftersom meddelanden i vanliga fall skickas från spelcentralens e-postadress.

6.6 Att avbryta en övning

I vissa fall blir man tvungen att avbryta en övning, till exempel om organisationen råkar ut för en verklig kris mitt under en pågående övning. Då kan man använda lösenordet ”skarpt läge” för att kommunicera att problemet som hanteras inte hör ihop med övningen.

I övningens dokumentation ska sådant som rör avbrytandet av övningen antecknas. Man fortsätter i allmänhet inte en övning som avbrutits, eftersom avbrottet stör koncentrationen på övningens innehåll. Deltagarna kan blanda ihop verkliga händelser och övningshändelser och övningens slutresultat blir lidande.

6.7 Modellering av övningsmiljön

Med simulering eller modellering av övningsmiljön menas att verkliga funktioner och resurser presenteras i spelets kontext på ett så trovärdigt sätt som möjligt. Till exempel kan mediekällor eller sociala medier modelleras med ett ändamålsenligt program eller genom att göra upp en visuell version.

Modellering av offentlig kommunikation är rätt okomplicerad eftersom kommunikationen i regel är enkelriktad. Till exempel behövs inga tekniska lösningar för att göra upp ett pressmeddelande i en skrivbordsövning. I en operativ övning kan spelcentralen ta emot de meddelanden som deltagarna gjort upp och skapa input utifrån dessa.

Modellering av media, och i synnerhet sociala medier, kräver däremot en teknisk miljö. Olika övningssimulatorer lämpar sig för detta ändamål. Via dessa är det möjligt att kommunicera i sociala medier och modellera även annan kommunikation. Olika program för direktmeddelanden och publikation fungerar också om man kan använda dem kreativt och tillämpande.

I en teknisk övning simuleras en teknisk verksamhetsmiljö där övningshändelserna huvudsakligen genomförs. Det finns flera övningsplattformar på marknaden där servrar och arbetsstationer modelleras på plattformen. Ofta finns det olika slags färdiga övningar på plattformen som det kan löna sig att bekanta sig med.

För att ordna en teknisk övning krävs simulering med olika system för att skapa en övningsmiljö, men även i en operativ övning kan man använda en simulator för att utveckla spelstoryn. Med hjälp av simulatorer kan man säkerställa att deltagarna får de uppgifter de behöver i övningen till sitt förfogande samtidigt.

Det finns färdiga lösningar på marknaden just för att simulera en övning. Man kan bygga en enkel övningssimulator till exempel på en gratis www-publikationsplattform där man skapar tidsinställda input i form av artiklar. Däremot saknar en sådan lösning egenskaper särskilt avsedda för övningsbruk som de övningssimulatorer som finns på marknaden har.

6.8 Lagen i en teknisk övning

I stora samövningar där man spelar i en teknisk miljö används i allmänhet färgkoder för att ange de olika lagens roller och uppgifter. De vanligaste lagfärgerna är röd, blå, vit och grön. Även lila, gul, grå eller andra färger kan användas beroende på spel och behov. De uppgifter som hör ihop med färgkoderna definieras i allmänhet i övningsdokumentationen eftersom det bortsett från rött eller blått inte finns någon standardiserad internationell tolkning av färgdefinitionen.

Enligt gängse praxis är det blåa laget de egentliga deltagarna. I stora samövningar kan

det finnas flera blåa lag. I dessa situationer kan de blå lagen tävla mot varandra om poäng som man samlar in genom att lyckas försvara systemet.

Det blå lagets motståndare är det röda laget. Det röda laget har till uppgift att sträva efter sina på förhand uppställda mål, till exempel att få åtkomst till och ta kontroll över det tekniska system som det blå laget skyddar.

Det röda lagets uppgift är att skapa en utmaning för det blå laget som anpassas efter försvararnas åtgärder och motaktioner. Det röda lagt består i allmänhet av övningsarrangörerna eller tekniska sakkunniga som arrangörerna särskilt bjudit in.

Övningsarrangörerna, de deltagande lagens kontaktpersoner, spelcentralen eller personer som företräder andra speladministratörer utgör det vita laget. Det gröna laget ansvarar för att upprätthålla nätverket och spelets infrastruktur och tillhandahålla teknisk support under spelets gång.

7 Analys av övningen – att dra nytta av lärdomarna

Man får ut största möjliga nytta av en övning om den analyseras noggrant. Här spelar observatören en central roll. Genom att avslutningsvis kombinera anmärkningar från deltagare, arrangörer och observatörer får man en mångsidig bild av övningen som man kan använda som grund för det framtida utvecklingsarbetet. Man kan med fördel se analysskedet som övningens viktigaste fas.

Förutom att man i analysfasen identifierar utvecklingspunkter, antecknar man även konkreta åtgärder för att ta sig an utvecklingspunkterna i övningen. Det är bra att göra en tidtabell för åtgärderna och följa upp dem så att de säkert genomförs.

Själva övningshändelsen ökar kunskapen om att hantera kriser och incidenter, men beklagligt ofta stannar denna kunskap hos ett fåtal personer. För att hela organisationen ska dra nytta av lärdomarna krävs det verkliga förändringar i verksamheten. Det är bra att komma ihåg att redan i övningens planeringsskede kan man göra observationer utifrån vilka organisationens verksamhet kan utvecklas.

När man ställer upp målen för övningen bedömer man vilken verksamhet som ska utvecklas under övningen. Antagandet kan stämma eller så kan övningen föra fram helt nya och överraskande kanaler och föremål för utveckling.

Bägge slutresultaten är nyttiga. Målen ska styra planeringen av övningen, inte begränsa den nytta den kan ge.

Genast efter övningen ordnas ett responstillfälle där deltagare och arrangörer kan föra fram sina första intryck och åsikter om övningens framgång. Samtidigt kan man samla in åsikter om själva arrangemangen kring övningen och bryta spänningen i övningssituationen. Ofta har deltagarna också frågor som de inte har kunnat ställa under övningens gång. En representant för spelcentralen bör vara beredd på att svara på deltagarnas frågor om genomförandet av övningen, dess story och bakgrund samt motivera de val som gjorts i övningen.

Det är bra att också be om skriftlig respons från deltagare och arrangörer. Fritt formulerad respons eller en blankett där man även numeriskt kan bedöma övningsupplevelsen lämpar sig bra för detta ändamål.

Observatörerna förmedlar sin respons renskriven till övningsarrangörerna. Om man har skapat en responsenkät kan den användas flera gånger och på så vis samlar man in information till en ”svarsbank” om den utveckling som skett mellan övningarna.

Sammanställda lärdomar och åtgärdsförslag delas ut till deltagarna för kännedom. När det visar sig att man med hjälp av övningen har hittat utvecklingspunkter och att man kommer att ändra praxis utifrån dessa, skapar det även motivation att delta i framtida övningar.

När lärdomarna har gjorts till en del av organisationens vardag tas de i beaktande i nästa övning. Det är till exempel bra att testa en utvecklad process igen under andra omständigheter och utmaningar för att se om utvecklingsriktningen är rätt eller fel. Även en fungerande process lämpar sig för ett övningsscenario för att på så sätt kunna anpassas att bli ännu bättre.

Med hjälp av en övning försöker man hitta svagheter hos processer och handlingssätt, inte hos människor. Det är viktigt att man inte upplever starka personliga misslyckanden i övningen. Deltagarna ska ges mod att tryggt våga prova djärva lösningar i övningen – även i kaotiska situationer.

Positiva erfarenheter är viktiga för den fortsatta övningsverksamheten. När deltagare klarat sig riktigt bra är det skäl att lyfta fram deras framgångar i samband med responssituationen.

7.1 Planering av responsenkäten

Samla in respons med ett verktyg avsett för en responsenkät. Bland annat webbläsarbaserade verktyg lämpar sig väl för detta. Med hjälp av verktyget kan man enkelt upprepa samma enkät även vid nästa övning och samtidigt bedöma hur övningsverksamheten utvecklats. Med en enkät får man även mer tid för att ge respons och sammanställa observationerna. Den kan inte ersätta muntlig respons, men skriftlig respons lämpar sig bättre för vissa.

I vanliga fall ingår det en responsenkät i en övning som en utomstående aktör arrangerat. Enkäten innehåller frågor om övningsarrangemangen och organisationens hantering av störningssituationen. Det huvudsakliga syftet med enkäten är att samla in information om själva utredandet av cyberstörningssituationen och i andra hand om arrangerandet av övningshändelsen.

För många kan det kännas omöjligt att ge muntlig och kritisk respons inför deltagargruppen, men lättare att göra skriftligen. Ta emot kritik av övningen med ett öppet sinne och försök förstå vad responsen grundar sig på. Ofta kan man ta den fråga eller det fenomen som ligger bakom kritiken i beaktande i följande övning. Kritisk respons ger möjlighet att förbättra övningsverksamheten och är därför positivt.

Tydliga poäng för övningens olika delområden gör det lättare att bedöma helheten och gör det även möjligt att rapportera övningserfarenheter vidare med tydliga nyckeltal. Responsenkäten för en övning bör åtminstone innehålla följande delområden:

Respondentens roll i övningen
- arrangör, observatör, deltagare, andra stöduppgifter
- ledning, it-förvaltning, tjänsteproduktion, annan enhet.

Övningens praktiska arrangemang
- utrymmen
- tidtabell
- information
- servering.

Sättet på vilket övningen ordnades
- Hade deltagargruppen valts på rätt sätt?
- Var övningsmetoden lämplig?
- Var instruktionerna tillräckliga?

Spelinnehållet i övningen
- Var scenariot trovärdigt?
- Fick man tillräckligt med information om händelserna under övningens gång?
- Var bakgrundsbeskrivningarna trovärdiga och lämpliga för övningen?

Övningen utvecklar yrkeskunskapen (subjektiv bedömning)
- Kan presenteras i form av en rad påståenden: ”Jag upplevde att övningen var nyttig” etc.
- Var ledningen av situationen lyckad?
- Lyckades man utveckla befintliga processer för hantering av störningar?

Villighet att delta i kommande övningar
- ”Jag deltar gärna i övningar också i fortsättningen.”
- ”Jag rekommenderar övningar för mina kollegor.”
- ”Jag upplevde att övningen var intressant.”

Öppen respons om övningen
- ris och ros, utvecklingsidéer, fri respons.

När man samlat in responsen sammanställs den i en tydlig presentation där uppgifter som kan identifiera respondenterna har strukits. Responsen delas ut till dem som deltagit i övningen.

8 Övning som en del av cybersäkerhetshantering

Hur övningsverksamheten utvecklas påverkas av vem som ansvarar för den i organisationen. En cyberövning skiljer sig inte avsevärt från övningar om andra krissituationer, så om det redan finns erfarenhet och kunskap om övningar i organisationen, till exempel vid enheten för företagssäkerhet, lönar det sig att använda dessa i planeringen av en cyberövning.

Det är en god idé att vidareutveckla övningsverksamheten från sporadiska händelser till en central del av cybersäkerhetshanteringen. På så sätt kan man periodisera och testa organisationens cybersäkerhetsverksamhet och -kultur som är i ständig förändring. Genom övning kan man även stärka samarbetet mellan organisationens olika avdelningar.

Samma övningar behöver inte upprepas med några månaders mellanrum, utan olika övningstyper kan utgöra en serie under året och en tydlig helhet. Under ett år kan man till exempel passa in några skrivbordsövningar och en eller två operativa övningar. Med personalen kan man samtidigt öva till exempel simulerade nätfiskeangrepp med tätare intervaller. Om det är möjligt kan man under övningsåret även passa in deltagande i en större samövning.

Hur omfattande en organisations övningsverksamhet är beror givetvis på organisationens storlek och resurser. Mindre organisationer har färre möjligheter till övningar än större.

När man ordnar övningar lönar det sig även att utnyttja samarbetsnätverk. Olika sammanslutningar, nätverk för informationsutbyte eller expertgrupper kan genomföra en övning som spelas till exempel i samband med ett gemensamt möte eller seminarium. Vid mötet kan man även bereda en övning som var och en sedan spelar i sin egen organisation. Till sist kan man tillsammans gå igenom resultaten och jämföra dem. En cyberövning som spelas samtidigt över organisationsgränserna och som planerats tillsammans skapar utmärkta tillfällen att öva samarbete i omfattande störningssituationer.

De huvudsakliga målen för enskilda övningsår styrs utifrån de strategiska målen. Målen för enskilda övningar kan ha sitt ursprung i de huvudsakliga målen. På så sätt blir en övning inte isolerad från det övriga informationssäkerhetsarbetet, utan istället en central del av det.

Övningsverksamheten kan innehållsmässigt delas in i olika årsteman. Ett övningstema behöver inte vara ett egentligt cybertema eftersom samma övningsmetoder även kan användas för att öva olika kriser i den fysiska världen och affärsverksamheten. Ofta når konsekvenserna av problemen i en cyberstörningssituation längre än de egentliga it-systemen.

I bästa fall kan hela organisationen delta i regelbunden övning. Det är klart att it-förvaltningen och den högsta ledningen övar på olika sätt och olika saker, men i båda fallen är övningar betydelsefulla, viktiga och en del av en välplanerad hantering av cybersäkerheten.

8.1 Långsiktig planering

Det lönar sig att inleda planeringen av det kommande övningsåret i god tid genom att samla in huvudteman för det kommande året som överensstämmer med den önskade utvecklingsriktningen för organisationens cybersäkerhetsarbete.

En ämneslista och tidtabell för ett specifikt år, utifrån vilka man kan skapa en årsklocka för övningsverksamheten, kan i stora organisationer se ut till exempel på följande sätt:

Mars 2020,
skrivbordsövning
- ämne: långvarig funktionsstörning av produktionssystemet, test av reservmetoder
- deltagare: produktionschefer, linjeförmän, kommunikation.

Maj 2020,
teknisk övning
- ämne: identifiering av angriparens åtgärder och loggning i produktionssystemet
- deltagare: SOC, it-förvaltningen.

Juni 2020,
skrivbordsövning:
- ämne: en central leverantör lägger ner sin verksamhet eller säljer den utomlands
- deltagare: ledningen, kommunikation.

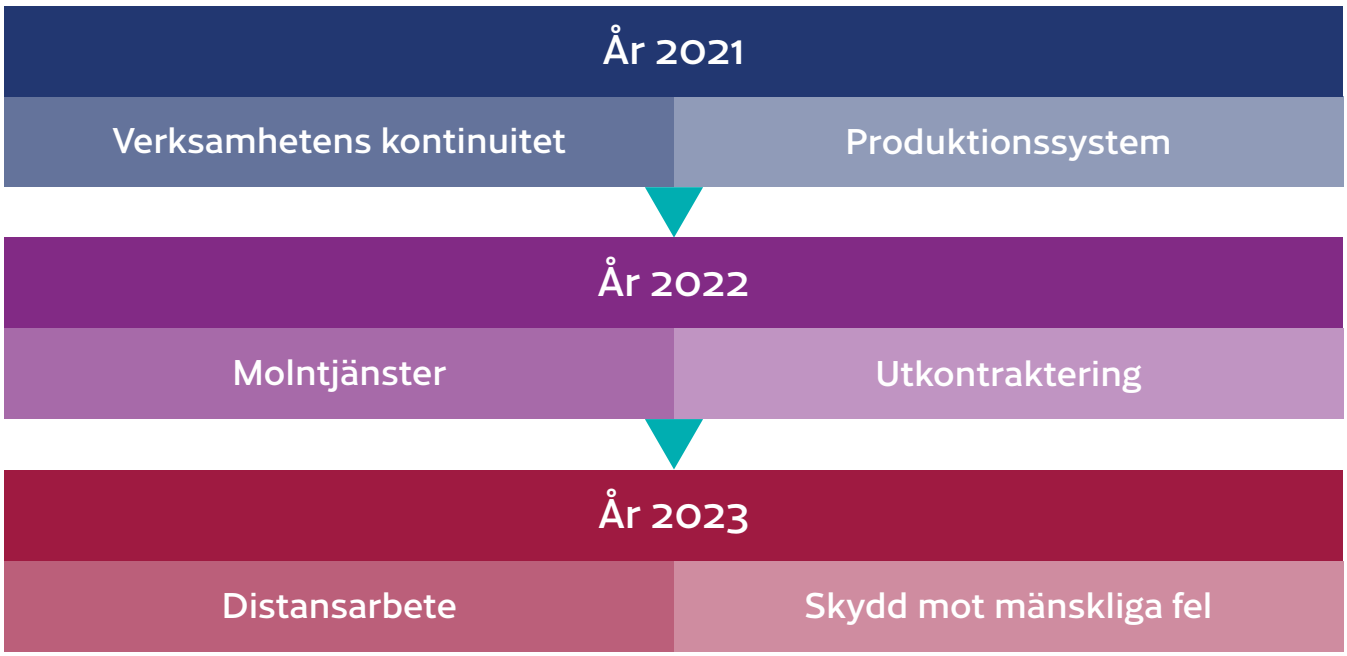
September 2020,
teknisk övning
- ämne: övning för att återställa säkerhetskopior
- deltagare: it-förvaltningen.

November 2020,
operativ övning för ledningen
- ämne: dataintrång i produktionssystemet, funktionsstörning, hur den inre kretsen utgör ett hot mot informationssäkerheten
- deltagare: ledningen, major incident, management-team, kommunikation.

I exempel X kretsar övningarna år 2021 kring att trygga och testa produktionssystemets driftssäkerhet. Övningarna har ett tematiskt samband, men deltagare från olika delar av organisationen deltar i dem. Övningsåret består av skrivbordsövningar, tekniska övningar och operativa övningar. Genom ett gemensamt tema stöder övningarna varandra och utgör en tydlig helhet. Vissa övningar går snabbt och enkelt att ordna, medan andra kräver lite mer tid. Att varva lättare övningar med tyngre möjliggör en mångsidig övningsverksamhet hela året. En regelbunden cykel håller de ämnen som tas upp i övningarna i färskt minne hela kalenderåret.

Till årets bärande tema kan man välja en abstraherad helhet såsom ”dataskydd” eller ”teknisk informationssäkerhet”. Organisationens eget riskhanteringsarbete, egen verksamhetsmiljö och förändringarna i den anger riktningen när teman ska väljas. Man kan skapa ett kontinuum för temana som inte är begränsat till ett år där övningsåren avlöser varandra på ett naturligt sätt. Årliga teman hjälper även att rikta informationssäkerhetsarbetet varvid informationssäkerhetsfrågor enligt temat bättre kommer fram.

Varje organisation gör upp sina egna årsspecifika mål och en egen övningscykel kring sin basverksamhet. I exemplet ovan har man valt ut två årsspecifika teman, men valen ska göras enligt egna behov. Årsspecifika teman kan vidareutvecklas till mål i enlighet med riktlinjerna i organisationens informationssäkerhetsstrategi.



9 Slutord

Vi hoppas att ni har nytta av den här anvisningen när ni i er organisation planerar och startar upp er cyberövningsverksamhet. Det är enkelt och okomplicerat att starta upp övningsverksamheten för med de enklaste övningsmetoderna kan man gå från idé till verklighet på ett par minuter.

Börja med enkla saker och fortsätt så småningom med mer komplicerade övningar. Innan ni vet ordet av är informationssäkerhetsårets höjdpunkt att komma på jävliga scenarier och fartfyllda intriger för en större övning.

Mer information om hur man ordnar en övning finns bland annat i följande allmänt tillgängliga verk:

- Handbook for planning, running and evaluating information technology and cyber security exercises (Center For Asymmetric Threat Studies, Swedish National Defence College, 2011)
- Exercise Guidance Basic Manual – An Introduction to the Fundamentals of Exercise Planning (Swedish Civil Contingencies Agency MSB, 2009)
- Manual and script for organizing cyber crisis exercises based on Cyber Crisis Exercise OZON (SURF Utrecht, 2017)
- Planning an Effective Incident Response Tabletop Exercise (Secureworks, 2018).

9.1 Kontaktuppgifter

Cybersäkerhetscentrets stödtjänster för övningsverksamhet står till de försörjningsberedskapskritiska organisationernas förfogande. Om ni är intresserade av att ordna er första cyberövning, hitta en lämplig samarbetspartner som stöd för er övningsverksamhet eller om ni behöver hjälp med att ordna en övning, ta kontakt med våra stödtjänster för övningsverksamhet på e-postadressen kyberharjoitukset@traficom.fi

9.2 Centrala begrepp

Övningshygien
Det sätt på vilket man säkerställer att övningens innehåll inte sprids utanför den grupp som deltar i övningen eller den lokal där övningen hålls. Se kapitlen 5.5 Utrymmen och 6.4 Kommunikation om övningen.

Övningsprogram
Det årliga program som organisationen gör upp som beskriver organisationens övningsverksamhet på en allmän nivå. I övningsprogrammet samlar man de övningar som ska planeras och spelas under året. Se kapitel 8.1 Långsiktig planering.

Övningssimulator
It-system som upprättats för att beskriva övningshändelserna och som används för att informera deltagarna om dessa. Se kapitel 6.7 Modellering av övningsmiljön.

Övningsscenario
En helhet som utgörs av händelserna i övningen och bakgrundsbeskrivningarna. Övningsscenariot beskriver innehållet i övningen. Kortfattat även ”scenario”.
Se kapitel 6.1 Övningsscenario.

Övningslag (t.ex. det blåa och det röda laget)
Olika färger används för att skilja mellan olika deltagare och arrangörer som har olika uppgifter i övningen. Används i synnerhet i tekniska övningar. Se kapitel 6.8 Lagen i en teknisk övning.

Övningstyp
Det spelsätt och den speltyp som valts för övningen.
Till exempel skrivbordsövning, operativ övning eller teknisk övning. Se kapitel 3 Olika typer av övningar.

Övningsmiljö
Den tekniska miljö där övningen genomförs. Övningsmiljön kan utgöras av antingen it-system eller företagets verksamhetsfält. Begreppet teknisk övning.
Se kapitel 3.4 Teknisk övning.

Hot wash-up
Responstillfälle som ordnas genast efter en övning.
Se kapitel 7 Uppföljning av lärdomarna av övningen.

Efteranalys
Insamling och granskning av lärdomarna från övningen efter att den genomförts samt omformning till praktiska åtgärder. Se kapitel 7 Uppföljning av lärdomarna av övningen.

Cyberövning
En säkerhetsövning som fokuserar på störningssituationer av it-system eller informationssäkerheten och de omfattande konsekvenser som följer av dessa i en organisation. Se kapitel 2 Vad är en cyberövning?

Spelare
Den egentliga deltagaren i en övning.
Se kapitel 5.2 Val av deltagare.

Spelcentral
Det utrymme varifrån ett pågående spel styrs och drivs framåt. Se kapitel 5.5 Utrymmen.

Pre-mortem
Grundorsaksanalys, en övning där man börjar med konsekvenserna och letar sig bakåt för att hitta möjliga grundorsaker. Se kapitel 3.2 Grundorsaksanalys.

Simulering
Beskrivning av de fiktiva händelserna i en övning.
Se kapitel 6.7 Modellering av övningsmiljön.

STARTEX, ENDEX
Kommandona för att inleda och avsluta en övning är ”start exercise” (starta övningen) respektive ”end exercise” (avsluta övningen). En övning inleds och avslutas med meddelandena STARTEX och ENDEX.

State of the world, bakgrundsbeskrivning av övningen
Bakgrundsberättelse som beskriver övningens utgångsläge. Kan användas för att skapa avvikande omständigheter för övningen. Se kapitel 6.3 Bakgrundsbeskrivningar.

Input (inject)
En enskild händelse, ett enskilt meddelande eller någon annan information som förmedlas till deltagarna och som för berättelsen framåt. Se kapitel 6.2 Input.

Inputtabell
En helhet som sammanställts av inputen i spelet som utgör övningens spelinnehåll. Se kapitel 6.2 Input.

Observatör
Övningsdeltagare som har till uppgift att observera övningen och anteckna sina iakttagelser i en promemoria.
Se kapitel 5.4 Stöduppgifter och observatörer.

Skarpt läge
Det uttryck som ska användas för att avbryta övningen då det föreligger ett verkligt problem eller tillbud.
Se kapitel 6.4 Kommunikation om övningen.

För mer information om cyber-säkerhet, kontakta oss via:
cybersakerhetscentret@traficom.fi

Transport- och kommunikationsverket Traficom

Cybersäkerhetscentret

PB 320, 00059 TRAFICOM
tfn 029 534 5000

traficom.fi

Transport- och kommunikationsverket
Cybersäkerhetscentret