Myndigheten för samhällsskydd och beredskap

Handbok

Tekniska informations- och cybersäkerhetsövningar

MSB:s kontaktpersoner:
Enheten för samhällets informationssäkerhet

Publikationsnummer MSB433
ISBN 978-91-7383-255-7

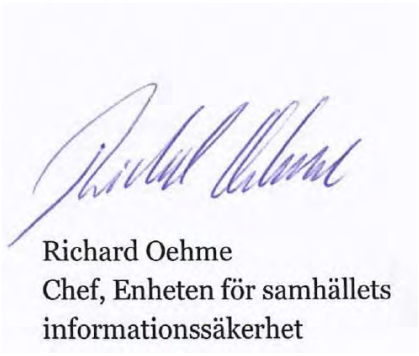
Förord

Informations- och cybersäkerhet kombinerat med färdighet i att kommunicera problem och lösningar i samverkan med andra och under påfrestande förhållanden kan förbättras genom övningar. Övningar – här specifikt *tekniska informations- och cybersäkerhetsövningar* – är ett komplement till organisationens ordinarie it-incidentrutiner samt övriga beredskaps- och krishanteringsövningar. De kan utföras i olika former och på flera sätt vilket denna handbok visar.

Handboken syftar till att vara en hjälp vid planering, genomförande och återkoppling av tekniska informations- och cybersäkerhetsövningar. Detta för att förbättra informations- och cybersäkerheten samt förmågan att hantera incidenter inom den egna organisationen, likväl som allvarliga IT-incidenter med påverkan på flera organisationer och samhället i stort.

I denna handbok har erfarenheter från tidigare tekniska informations- och cybersäkerhetsövningar införts. Handboken är ursprungligen framtagen vid Försvarshögskolan, Centrum för asymmetriska hot- och terrorismstudier (CATS) på uppdrag av Myndigheten för samhällsskydd och beredskaps (MSB). Den har därefter bearbetats vid MSB för att tillföra ytterligare erfarenheter och för att ligga i linje med myndighetens övriga dokumentation i frågan. Handboken är därvidlag skriven med utgångspunkt i Myndigheten för samhällsskydd och beredskaps (MSB:s) övningshandbok *Öva krishantering – Handbok i att planera, genomföra och återkoppla övningar* från 2009.

Denna handbok ska ses som ett komplement till MSB:s övningshandbok. Den är framför allt tänkt att vara en hjälp för aktörer inom informations- och cybersäkerhetsområdet generellt, och inom skydd av samhällsviktig informationsinfrastruktur mer specifikt. Handboken kommer efter några år att revideras och erfarenheter och synpunkter tas därför gärna emot.



Richard Oehme
Chef, Enheten för samhällets informationssäkerhet

Innehåll

Figurer och tabeller

Förkortningar och akronymer

BCS	Baltic Cyber Shield
CATS	Centrum för asymmetriska hot- och terrorismstudier
CCB	Configuration and Control Board
CCD COE	Cooperative Cyber Defence Centre of Excellence
CDX	Computer Distributed Exercise
CERT	Computer Emergency Response Team
DNS	Domain Name System
DMZ	Demilitariserad Zon
FHS	Försvarshögskolan
FMV	Försvarets materielverk
FOI	Totalförsvarets Forskningsinstitut
FRA	Försvarets radioanstalt
FTP	File Transfer Protocol
ISP	Internet Service Provider
IT	Informationsteknik
KBM	Krisberedskapsmyndigheten
MSB	Myndigheten för samhällsskydd och beredskap
NISÖ	Nationell informationssäkerhetsövning
OTRS	Open Technology Real Services
Peer-2-peer-nätverk	Ett datornätverk av sammankopplade noder som inte kommunicerar enligt klient-server-modellen
SCADA	Supervisory Control and Data Acquisition

1. Introduktion

Sveriges informations- och cybersäkerhetsaktörer finns inom såväl den privata som den offentliga sektorn i samhället. Det är dessa som ser till att data och information i system och nätverk är skyddad mot intrång och förstörelse samtidigt som den är tillgänglig för rätt personer vid rätt tillfälle.

Informations- och cybersäkerhetsarbetet pågår ständigt inom varje organisation. Förutom att säkerställa att den löpande verksamheten fungerar under normala omständigheter med vardaglig incidenthantering, ansvarar aktörer inom såväl privata organisationer som offentliga myndigheter samtidigt för att samhällets informationsinfrastruktur och skyddet av denna ska fungera vid allvarliga IT-incidenter.

Vid en allvarlig händelse med ökad påfrestelse på en organisation, en bransch eller större del av samhället, behöver även informations- och cybersäkerheten upprätthållas för att IT- och kommunikationssystemen ska kunna fortsätta att fungera, eller snabbt kunna återupptas i drift vid ett eventuellt uppehåll. I normalläge såväl som under extraordinära förhållanden behöver data och information kunna överföras utan att avkall görs för bristande konfidentialitet, riktighet och tillgänglighet.

Detta arbete sträcker sig från ordinarie verksamhet, till förberedelser för att kunna hantera en allvarlig IT-incident, faktisk hantering av händelsen när den inträffar och avslutas i efterarbetet med identifiering av lärdomar och uppföljning. För att informations- och cybersäkerhetsarbetet ska fungera behöver samtliga involverade, från såväl den egna organisationen som aktörer inom andra organisationer kunna samverka och kommunicera med varandra.

Informations- och cybersäkerhet kombinerat med färdighet i att kommunicera problem och lösningar i samverkan med andra och under påfrestande förhållanden, kan förbättras genom övningar. Det gäller särskilt där det ställs krav på beslutfattande under tidspress, påverkan på stora värden, egendomar och människors liv. Övning i hantering av storskaliga IT-incidenter med omfattande komplexitet, geografisk bredd och påverkan på lokal, regional och nationell nivå är därför av stor vikt. Inte minst då hantering av allvarliga IT-incidenter kräver samverkan utanför den egna organisationen och samhällssektorn.

Övningar – här specifikt tekniska informations- och cybersäkerhetsövningar – är ett komplement till organisationens ordinarie beredskaps- och krishanteringsövningar. De kan utföras i olika former och på flera sätt vilket denna handbok visar.

Handboken för tekniska informations- och cybersäkerhetsövningar är skriven med utgångspunkt i Myndigheten för samhällsskydd och beredskaps (MSB:s) existerande övningshandbok *Öva krishantering – Handbok i att planera, genomföra och återkoppla övningar* där gjorda erfarenheter från tidigare tekniska informations- och cybersäkerhetsövningar applicerats.[1] Denna handbok ska ses som ett komplement till MSB:s övningshandbok.

[1] MSB (2009) *Öva Krishantering – Handbok i att planera, genomföra och återkoppla övningar,* Myndigheten för samhällsskydd och beredskap. (Tillgänglig via: http://www.msb.se/RibData/Filer/pdf/25608.pdf, 2010-10).

1.1 Vad tekniska övningar kan bidra med

Övningar inom informations- och cybersäkerhetsområdet kan bidra till:

1. att öka samverkan, genom ökad förståelse för och vana av samverkan på myndighetsnivå likväl som mellan privat och offentlig sektor,
   - att deltagarna (yrkesverksamma i privat och offentlig sektor) kan utbyta erfarenhet och information med varandra, vilket i sin tur bidrar till ökad förståelse och kunskap mellan dem som ingår i övningen,
   - att öka förståelsen för den nationella och internationella cybermiljön med avseende på policy, juridiska aspekter samt behovet av internationell samverkan, samt
   - att utveckla och utöka den nationella och internationell samverkan i förmågan att hantera storskaliga IT-incidenter/cyberincidenter.
2. att hitta sårbarheter i övade/testade system,
   - att visa på önskvärda säkerhetsegenskaper i informationssystem för att till exempel kunna säkra och skydda sig mot olika former av skadlig kod såsom datavirus,- maskar och trojaner samt DDoS-attacker med mera,
3. att IT-incidenter och IT-attacker samt skydd av kritisk informationsinfrastruktur kan studeras och utvecklas,
   - att kunskapen om och färdigheten i att planera, genomföra och följa upp tekniska informations- och cybersäkerhetsövningar förbättras.
   - att testa it-incidentrutiner samt beredskaps- och krishanteringsplaner.

1.2 Syfte

Denna handbok syftar till att vara en hjälp vid planering, genomförande och utvärdering samt erfarenhetsåterkoppling av tekniska informations- och cybersäkerhetsövningar. Den är framför allt tänkt att vara en hjälp för aktörer inom informations- och cybersäkerhetsområdet generellt, och inom skydd av samhällsviktig informationsinfrastruktur mer specifikt. Detta för att förbättra informations- och cybersäkerheten samt förmågan att hantera incidenter inom den egna organisationen, likväl som allvarliga IT-incidenter med påverkan på flera organisationer och samhället i stort.

Handboken är främst inriktad på övningar med fokus på IT-säkerhet och administrativ säkerhet, samt de åtgärder som krävs för att skydda samhällsviktig data och information, datorer eller datorsystem/informationssystem i nätverk mot attacker och intrång. Boken är därtill en guide för övning i praktiken av åtgärder för att säkra, upptäcka och reagera på intrång i informations- och kommunikationssystem, d.v.s. informationssäkring. Informationssäkring omfattar såväl människors agerande, IT, och processer som policy på området.

1.3 Målgrupp för handboken

Handboken är främst tänkt att vara ett stöd för organisationers säkerhets- och övningsansvariga och andra som har ansvar för ledning och styrning inom informations- och cybersäkerhetsområdet. Handboken kan samtidigt läsas av såväl övningsdeltagare som andra intresserade av informations- och cybersäkerhetsövningar.

1.4 Avgränsningar

Handboken rör sig mellan den nationella ledningsnivån (övre gräns) till driftsansvariga för IT- och nätverkssäkerhet (undre gräns) i såväl privata som offentliga organisationer. Den sträcker sig på det tekniska planet till att tydliggöra för övningsägare och övningsledare vad dessa bör kunna ställa för krav beträffande tekniska specifikationer, sekretessaspekter med mera gentemot leverantörer av den tekniska miljön som är nödvändig för att kunna genomföra informations- och cybersäkerhetsövningar.

Handboken är inte allomfattande eller avser ge en uttömmande bild av hur tekniska informations- och cybersäkerhetsövningar kan eller ska planeras, genomföras eller återkopplas. En informations- och cybersäkerhetsövning är en aktivitet som till sin natur är avgränsad i tiden och bör därför genomföras i projektform. Denna handbok behandlar dock inte projektstyrningsprocessen eller ger rekommendationer om projektledningsmodeller.

Genomförande av övningar i form av workshops, seminarier och som skrivbordsövningar omfattas inte av denna handbok.

Att notera är att samtidigt som referenser till cyberförsvar och cyberförsvarsövningar (Cyber Defence Exercises) förekommer i texten är detta inte inriktningen för denna handbok och kommer därför inte att beskrivas ytterligare.

1.5 Metod

Handboken bygger på en expertbetonad metodansats, kvalitetsgranskad genom dialog med enskilda experter och en workshop med deltagare med erfarenhet från tidigare arbete med informations- och cybersäkerhetsövningar nationellt och internationellt. Bakgrunden och materialet till boken är baserad på praktiska erfarenheter från projekt- och övningsledare samt övningsdeltagare och därtill referenser och projektrapporter från tidigare genomförda övningar.

Erfarenheter redovisas från de simulerade övningarna Cyber Defence Exercise2 2008 (”CDX-I”), Baltic Cyber Shield 2010 (”CDX-II”) samt CDX-2012/MNE7 ”Locked Shields” (”CDX-III”). Dessutom har erfarenheter från seminarieövningen Nationell informationssäkerhetsövning (NISÖ) 2010 och 2012 tagits i beaktande och detsamma gäller för en informations-säkerhetsövning i skarpa system genomförd några år tidigare.

1.6 Definitioner och centrala begrepp

- *Storskalig IT-attack/ storskalig säkerhetsincident i nätverk*[3]*/ allvarlig IT-incident/cyberincident:* här avses IT-relaterad händelse (där IT ses i vid bemärkelse) som bidrar till en allvarlig störning i samhällsviktig verksamhet, eller kris för samhället, då denna är av omfattande geografisk bredd med påverkan på lokal, regional och nationell nivå, vilket kräver snabba insatser och samverkan utanför den egna organisationen.
- *Extraordinär händelse:* en ”händelse som avviker från det normala, innebär en allvarlig störning eller överhängande risk för

[2] Även kallad Computer Distributed Exercise.
[3] Se ”Skydd mot storskaliga IT-attacker och avbrott: förbättrad beredskap, säkerhet och motståndskraft i Europa”, EG-kommissionen, KOM(2009) 149 slutlig. Bryssel den 30 mars 2009, s. 10.

en allvarlig störning i viktiga samhällsfunktioner och kräver skyndsamma insatser av en kommun eller ett landsting."[4]

- *Samhällsviktig verksamhet*: "definieras som en samhällsfunktion av sådan betydelse att ett bortfall av eller en svår störning i funktionen skulle innebära stor risk eller fara för befolkningens liv och hälsa, samhällets funktionalitet eller samhällets grundläggande värden."[5] Exempel är "el- och vattendistribution samt spårbunden trafik och petrokemisk industri".[6]
- *Informationssäkerhet*: är ett övergripande begrepp som omfattar såväl fysisk säkerhet (skydd av lokaler, medarbetare m.m.), data-/IT-säkerhet (skydd av servrar, data och kommunikation via e-post m.m.) som administrativ säkerhet (policy, kontinuitetsplaner, regelverk m.m.).[7]
- *Cybersäkerhet* följer av informationssäkerhet ovan samtidigt som det inkluderar åtgärder för skydd av data, datorer eller datorsystem i nätverk (Internet) mot intrång och attacker.[8]
- *Teknisk informations- och cybersäkerhetsövning:* här avses övning med inriktning på en organisations IT-system i nätverk i relation till andra processmässiga (operationella, rättsliga och policyrelaterade) aspekter vid händelse av en allvarlig IT-incident.
- *Informationssäkring* (*Information Assurance*, IA): Begreppet är mer specifikt inriktat på praktiken (hur), det vill säga "åtgärder i fred, kris eller krig för att säkra civil och militär information samt informations- och kommunikationssystem av vital betydelse för samhällets säkerhet"[9]. IA omfattar även åtgärder för att upptäcka och reagera på exempelvis intrång samt åtgärder för att återställa informationssystem.

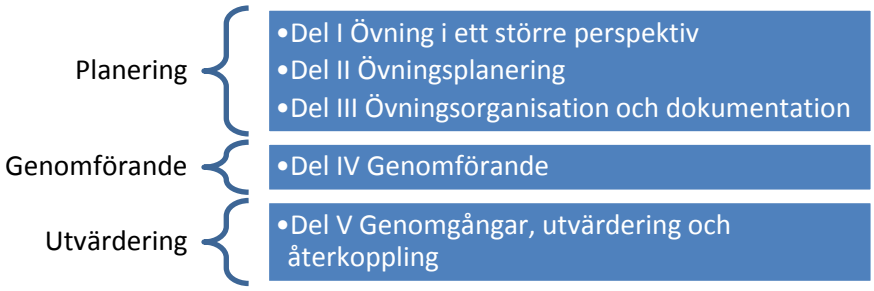
1.7 Disposition

Handboken bygger på en övningsplaneringsprocess i tre steg. Dessa är:

1. Planering
2. Genomförande
3. Utvärdering

Nedanstående figur visar hur denna handboks disposition täcker avsnitten I till V i MSBs övningshandbok.

[4] 1 kapitlet 4 § i lag (2006:544) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap (LEH).
[5] MSB, Ett fungerande samhället i en föränderlig värld, Nationell strategi för skydd av samhällsviktig verksamhet. DanagårdLiTHO, MSB266, Maj 2011.
[6] MSB, Strategi för samhällets informationssäkerhet, 2010-2015. MSB, Karlstad: 2010.
[7] SIS, *Terminologi för informationssäkerhet*, SIS HB 550, utgåva 3. SIS Förlag AB, Elanders: 2007.
[8] Merriam Webster, via http://www.merriam-webster.com/dictionary/cyberssecurity, 2011-02-09.
[9] SIS (2007), s. 73.



Figur 1 Disposition och relation till MSBs övningshandbok.

2. Planering

Nedanstående avsnitt behandlar de inledande aktiviteterna som måste ske före genomförandefasen, d.v.s. förberedelser och planering.

Läsanvisning
MSB:s övningshandbok Del I-III

2.1 Inventering och behov av övning

2.1.1 Initiativ och uppdrag

Innan övningsplaneringen startar bör riktlinjer och avgränsningar för övningen och övningsplaneringsprocessen vara tydligt formulerade och förankrade. Det ska finnas en tydlig uppdragsgivare på vems initiativ övningen sker samt en fastställd budget för det tilltänkta övningsprojektet omfattande hela planeringsprocessen från planering och genomförande till återkoppling, samt bland annat tydliggöra behov av personal, resor och teknik.

2.1.2 Behovsanalys – varför ska vi öva?

Innan övningsplaneringen tar vid ska även behovet av en övning vara tydligt formulerat. En behovsanalys, till exempel i form av en risk- och sårbarhetsanalys av en viss funktion, del av eller hela verksamheten kan vara behjälplig för detta. Även tidigare övningar kan tydliggöra behov för ny övning som antingen en enstaka insats eller som flera övningar i en serie.

Behovsanalysen bör belysa organisationens/verksamhetens och den enskildes uppgift, förändringar i organisationen/av verksamheten, erfarenheter av tidigare övningar och verkliga händelser, samt nuvarande förmåga (kunskap, skicklighet) hos de övade att kunna utföra sina uppgifter.

Vidare bör analysen ge svar på följande frågor:

- Vad ska övningen uppnå? – Övergripande syfte med övningen.
- Vilka ska övas? – Övningens målgrupp för vem syfte och mål med övningen senare ska specificeras.
- Vad ska övas? – Valet av övningstyp och innehåll.
- När ska man öva?
- Hur ska man öva? – Valet av övningsform och praktiskt tillvägagångssätt/metod för genomförande av övningen.
- Var ska man öva?
- Vilka resurser behövs?

Utifrån behovsanalysen tydliggörs såväl ’varför vi ska öva’, som omfattning och metod för övningen.

2.2 Flerårig övningsplan

För att få kontinuitet i övningsverksamheten bör en flerårig övningsplan tas fram. Denna bör i sin tur bygga på en kompetensutvecklingsplan för organisationens medarbetare. Övningsplanen är en tabell som i kronologisk ordning visar vilka övningar som avses genomföras och när dessa är tänkta att äga rum. Den visar samtidigt vilka funktioner inom en organisation, eller inom vilka olika organisationer, som avses övas vid de olika tillfällena, samt när utvärdering, återkoppling och uppföljning ska vara genomförda.

Beaktande omloppstiden (från planering och genomförande till återkoppling) för tekniska informations- och cybersäkerhetsövningar och att övningsplanen inkluderar flera olika övningar, bör den omfatta en flerårsperiod och gärna sträcka sig över tre till fem år. Övningsverksamhet som struktureras på detta sätt blir även enklare att överblicka och vägen till målet blir tydligare.

Övningsverksamheten kan till exempel åskådliggöras i form av en utvecklingstrappa där informations- och cybersäkerhetsövningarna blir mer avancerade och komplexa,[10] involverar fler funktioner eller delar inom en organisation, eller inom fler och olika organisationer inom ett större samverkansområde.

Övningsplaner som sträcker sig över flera år kan skrivas för såväl en samhällssektor, till exempel energiförsörjning, kommunikation och transport etc., en region, eller en organisation (företag, myndighet). Övningsplanen bör, i likhet med en projektplan, innehålla:

- mål för övningsverksamheten
- tidsplan
- ansvarsförhållanden och
- beräknade resurser (ekonomi, personal och kompetenser, teknik och materiel etc.).

Med avseende på den sista punkten ”resurser” ovan är det viktigt att tidigt planlägga resurserna personal/kompetens, teknik/material samt ekonomi. Dessa har ett avgörande inflytande på övningsplaneringsprocessen från planering till genomförande och uppföljning.

Ekonomin, framför allt kostnaderna, för övningen bör budgeteras för redan under planeringsfasen. Detta så att ambitionsnivåer kan väljas. Dels för att besluta om övningens mål och omfattning, dels för att kunna göra förändringar under genomförandet om de ekonomiska förutsättningarna skulle ändras och dels för att kunna göra utvärdering och uppföljning av övningsresultatet.

I utvärderingsfasen ingår även att dokumentera de ekonomiska utfallen på ett sådant sätt att materialet kan användas vid planering av en ny/efterkommande övning. Samtidigt som den fleråriga planen ger övningsansvariga ett sätt att strukturerat åskådliggöra för ledning och beslutsfattare hur planerade informations- och cybersäkerhetsövningar också passar in i organisationens övnings- och kompetensutvecklingsplan, samt strategi för detta, är den alltid att betrakta som ett levande dokument.

[10] Inom ramen för Sveriges deltagande i tidigare internationella tekniska laborationsövningar på informationssäkerhetsområdet (s.k. Cyber Defence Exercises, CDXs) har det övergripande målet varit att lära mer om genomförandet och hur denna form av övningar kan sättas upp.

2.3 Övning som lärandeprocess

Oavsett målet med övningen är den alltid att betrakta som en lärandeprocess för såväl övningsplanerare som de övade. En lärorik övning för vissa kan vara en stressande och ångestfylld erfarenhet för andra. Samtidigt som tekniken och metoden för övningen lätt hamnar i fokus, bör även den mänskliga aspekten uppmärksammas i övningsplaneringen. Detta omfattar bland annat en god atmosfär genom hela övningsplaneringsprocessen för att deltagarna ska känna sig väl bemötta och engagerade.

Vid utformningen av en övning, om än beroende av dess syfte och mål, kan övningsdeltagarna involveras genom att tillfrågas om vilken kunskap eller färdighet inom informations- och cybersäkerhetsområdet de vill förbättra genom övning. Det är även viktigt att övningens svårighetsgrad är anpassad till rådande tekniska förutsättningar och deltagarnas färdighetsnivå.

2.4 Om övningsplanering

Ett första steg i övningsplaneringen är att bestämma övningens syfte, övergripande mål och avgränsningar. Denna del i planeringen bygger på tidigare fastställda direktiv och dialog där syftet tydliggjorts samt möjligen även mål, målgrupp och avgränsningar diskuterats. Det är emellertid här den egentliga målformuleringen eller processen för att bestämma mål, den så kallade målsättningen sker.

Under detta steg i övningsplaneringsprocessen bör även behovet av externa resurser, till exempel konsulter, och samarbete med andra parter för övningsplanering, genomförande och utvärdering samt återkoppling tas med i beaktande. Detta för att i tid dels kunna beställa extra resurser som kan ha begränsad tillgänglighet som till exempel personer/konsulter och teknik, men även för att omfatta tidsåtgång för eventuellt upprättande av avtal och överenskommelser med andra parter.

Anledningen till varför en informations- och cybersäkerhetsövning anordnas och genomförs kan variera och likaså syftet. Exempel på syften med övningen kan vara att:

- ”*utbilda* genom att *lära ut* något nytt till de övade – individer eller organisation ska ges möjlighet att få ökade kunskaper och färdigheter
- *pröva* ny organisation, ny teknik med mera och därmed upptäcka styrkor och svagheter
- förutsättningslöst *utveckla* verksamheter genom att till exempel öva samverkan eller kommunikation med omvärlden
- *mäta* förmågan och uthålligheten.”[11]

En av de erfarenheter som övningsledningen för NISÖ 2010 och Cyber Storm III ansett vara särskilt viktiga att föra vidare i planeringsprocessen för NISÖ 2012, var att gå mer mot prövande informations- och cybersäkerhetsövningar.[12]

”Rutiner och arbetsformer inom området utvecklas ständigt så lärande övningar spelar fortfarande en viktig roll. Det är dock viktigt att öka de prövande inslagen och realismen. Prövande inslag ”tydliggör och sätter problem på kartan”. Fler prövande inslag i övningar kan även vara ett sätt att driva utvecklingen av gemensamma ramverk för samverkan samt

[11] MSB (2009), s. 21. Författarnas kursivering.
[12] Se rapporten *Nationell informationssäkerhetsövning 2010 (NISÖ 2010) och Cyber Storm III – Sammanställning av slutsatser och erfarenheter som underlag för planering av NISÖ 2012,* Dnr. 2011-3592, MSB, 2012.

processer och rutiner för hantering av allvarliga IT-incidenter. Vissa aktörsgrupper är redan idag mogna för prövade inslag och olika aktörsgrupper kan ha olika grad av prövade element i en och samma övning".

Målen med övningen kan delas upp i huvudmål och delmål genom att övergripande mål bryts ned i mer specifika delmål. Mål ska fram för allt vara mätbara. Därtill finns en utvidgad minnesregel för att skapa tydliga och uppföljbara mål vilken beskriver att mål ska vara "SMARTA", det vill säga:

- Specifika – tydligt avgränsade
- Mätbara – detaljerade
- Accepterade – godkända av uppdragsgivare/beställare, övningsledning och utvärderare
- Realistiska – rimliga och möjliga
- Tidsatta – tidpunkt finnas för när resultat/förmåga ska ha uppnåtts
- Adekvata – lämpliga i förhållande till syftet.

Vid målformuleringen kan aktivitetsverb vara behjälpliga i beskrivningen av vilka resultat övningen ska utmynna i. Dessa kan till exempel vara "att känna till", "att behärska" etc. Det är samtidigt viktigt att konkretisera vad som menas med "känna till", "ha kunskap om" eller "god förmåga till" för att fastställa kriterier för bedömning av förmågan vid utvärderingen i senare skede.

Målgrupp är de individer eller grupper, enheter eller dylikt som avses övas utifrån tidigare uppställt syfte och mål. En övning kan vända sig till flera olika deltagare – till exempel It-tekniker och säkerhetsansvariga samt jurister och organisationens ledning, eller såväl övade på olika platser inom en organisation samtidigt som övningsledningen – och således ha flera målgrupper. Det bör dock tydligt framgå vilka mätbara mål som riktar sig till vilken/vilka målgrupp/-er för att möjliggöra utvärderingen.

Avgränsningar för övningen är sådant den i förväg inte avser omfatta eller uppnå. För tekniska informations- och cybersäkerhetsövningar kan det till exempel innebära att när man avser öva organisationens interna incidenthantering kan övningen avgränsas till att endast öva vissa system och inte alla samtidigt.

Tänk på att:

- genomföra en grundlig behovsanalys innan övningsplaneringen tar vid. Denna ska bland annat besvara vad övningen är tänkt att uppnå, vem och vad som ska övas, när var och hur, samt vilka resurser som behövs.
- göra en flerårig övningsplan – gärna på mellan tre till fem år – som inkluderar omloppstiden för tekniska informations- och cybersäkerhetsövningar och även inkluderar flera olika övningar. För detta arbete är det viktigt med tydliga mål, tidsplaner och ansvarsförhållanden för övningsverksamheten samt inte minst att resurser beräknas för planläggande och budgetarbete utmed hela övningsplaneringsprocessen.
- ha ett skriftligt direktiv från uppdragsgivaren/beställaren vilket kan analyseras i en dialog innan övningsplaneringen tar vid.
- beakta och beräkna behovet av externa resurser (till exempel konsulter) samt tidsåtgång för eventuellt upprättande av avtal och överenskommelser med andra parter (organisationer, myndigheter och företag).

2.5 Övningsformer och övningstyper

Vid val av metod för övningen, det vill säga övningsform och övningstyp, är det viktigt att utgå från syftet och målet/-en med övningen. De övningsformer för informations- och cybersäkerhetsövningar som denna handbok omfattar, är:

- simuleringsövning, samt
- skarp övning i existerande system i realtid.

Båda övningsformerna kan antingen genomföras på en och samma plats eller som en distansövning (distribuerad övning). Övningsformerna kompletterar varandra och en övning kan ha inslag av olika former, om detta är lämpligt för att uppnå övningens syfte och mål.

2.5.1 Simuleringsövning eller laborationsövning med motspel

Simulering eller spel är en övningsform som i så stor utsträckning som möjligt sker i en miljö och med uppgifter som liknar verkligheten vid en kris orsakad av en allvarlig IT-incident. I fallet med informations- och cybersäkerhetsövningar genomförs övningarna med fördel i en konstruerad, fiktiv spelmiljö, där infrastrukturen sätts upp separat från organisationens ordinarie IT-miljö.

2.5.2 Skarp övning

Skarp övning, även kallad praktisk övning, genomförs i verklig miljö. En skarp informations- och/eller cybersäkerhetsövning genomförs i den existerande organisationens egna system och med de resurser som skulle användas vid en allvarlig IT-incident och verklig kris, eller för att testa och finna sårbarheter i egna system samtidigt som andra organisatoriska funktioner och till exempel ledningen övas parallellt.

För denna övningsform är det om än ännu viktigare att syfte och mål med övningen förankrats hos uppdragsgivaren och att tid och resurser läggs på att informera och instruera de övade och andra berörda om vad de kan och får göra för att inte störa den ordinarie verksamheten.

2.5.3 Simulering eller skarp övning?

Enligt MSBs handbok för övningar, är simuleringsövningen ”främst lämplig om målet är att pröva funktioner, organisation, samverkansformer etc. Den kan även användas för det som seminarieformen kan användas för. En erfaren organisation som tidigare övat mycket kan välja simuleringsövning med motspel. Detta kräver vanligtvis att organisationen är väletablerad, det vill säga att struktur, roller, uppgifter med mera är tydliga och väl förankrade.”[13]

Den *skarpa övningen* bör användas med viss försiktighet för att inte störa den ordinarie verksamheten. Den används fram för allt för att för att testa organisationens existerande system och rutiner för att finna sårbarheter och svagheter i säkerheten hos dessa. Övningsformen kräver mycket god planering och noggranna förberedelser för att inte försätta organisationen i en kompromettерande situation där hela informationssystem eller delar av dessa stängts av eller tagits ner på grund av övningen.

2.5.4 Rött lag/Blått lag-övning

För informations- och cybersäkerhetsövningar används ofta en övningstyp benämnd *Red Team/Blue Team Exercise* (Rött lag/Blått lag-övning). Denna övningstyp lämpar sig för samtliga övningsformer (seminarium, simulering och skarpa övningar) och är fram för allt att föredra vid simuleringar eller

[13] MSB (2009), s. 33-34.

laborationsövningar på grund av dess flexibilitet och möjlighet att stödja olika målsättningar med en informations- och cybersäkerhetsövning.

Namnet på övningstypen har sitt ursprung i militärens test av beredskap för strid. Övningsupplägget är normalt sådant att två grupper/lag spelar mot varandra. Ett rött lag, till exempel bestående av säkerhetsprofessionella ”etiska” hackare, attackerar det blå (försvarande) lagets informationssystem. Det blå laget har till uppgift att skydda sina system och upptäcka intrång och allvarliga incidenter eller sådana som kan eskalera. Övningstypen har även använts för att testa fysisk säkerhet inom samhällsviktig infrastruktur som kärnkraftverk och högteknologiska laboratorier. Under 1990-talet började experter att använda övningstypen för att testa säkerhet i informationssystem.

Rött lag/Blått lag-övningar kan emellertid ha en rad olika konstellationer. Till exempel kan en övning bestå av flera blå lag som antingen var för sig eller tillsammans samarbetar för att skydda sina system mot ett eller flera attackerande röda lag. En övning kan även bestå av endast blå lag (ett eller flera), utan något rött motspelslag, med uppgift att skydda sina system, upptäcka intrång och rapportera incidenter.

Det är även möjligt att sätta upp så kallade dubbelsidiga övningar där två eller flera lag attackerar varandra och samtidigt behöver skydda sina egna system. För denna sammansättning är det om än ännu viktigare att från projektledningen och övningsplaneringens sida tydliggöra syftet och målen med övningen. Då det ofta är otydligt vad som övas med denna specifika sammansättning är den inte att föredra.

Övningar av typen Rött lag/Blått lag är flexibla i det att de även kan modifieras beroende på lagens kännedom om det eller de system de övar i. Deltagarna kan således antingen gå in i övningen utan kännedom om systemet eller systemen de ska öva inom, alternativt ha god kännedom om dessa eller något däremellan. Övningsmetoden för lagens kännedom om systemet eller systemen under övningen brukar ibland refereras till som *White-box* med full kännedom och insyn i systemen före övningen, eller *Black-box* utan kännedom om systemen före övningen.

2.6 Övningstider

Under den inledande övningsplaneringen och i samband med valet av övningsmetod – form för och typ av övning – är det även viktigt att fastställa tid för genomförandet av övningen, planeringsmöten, genomgångar med mera. I direktivet framgår syftet med övningen och tillsammans med målen och avgränsningarna utgör dessa ramar för valet av övningsform och övningstyp samt till del även övningstiden.

Planeringstiden och således även tiden för genomförande och återkopplingen av informations- och cybersäkerhetsövningar är relativt lång för såväl simuleringar som för skarpa övningar. Givet tillgång till den tekniska infrastrukturen (övningsmiljön) för simulerings-/laborationsövningar och även skarpa system om denna form väljs, blir förberedelse- och planeringstiden givetvis kortare för varje gång en övning initieras till dess att endast mindre justeringar behöver göras och mer tid faktiskt går åt till planering, framtagande av scenario med mera.

Viktigt är dock att i god tid under den övergripande planeringen diskutera och fastställa:

- faktisk tid för genomförandet av övningen (hur länge övningen ska löpa; en, två eller fler dagar; endast dagtid, kvällstid eller dygnet runt, vardag eller helgdag etc.).

- virtuell/spelad tid under genomförandet av övningen. Detta hänger samman med övningsscenariots upplägg och vad som är tänkt att ske inom ramen för övningen. Det är troligt att övningens syfte och mål ställer sådana krav på upplägget av övningen att en uppdelning blir nödvändig i olika faser. Vid en fasindelning möjliggörs tidshopp under övningen, vilka i sin tur kan vara kända eller okända för övningsdeltagarna/de övade.
- tid för genomgångar under övningen och för återkoppling efteråt, samt
- synkroniserad tid (tidzon och faktisk tid) för samtliga system under genomförandet av övningen.

En synkroniserad tid är fram för allt viktig för laborationsövningar (distribuerade eller inte spelar mindre roll), samt skarpa övningar med flera arbetsstationer och system involverade.

2.7 Planeringsorganisation

MSBs övningshandbok anger att "planeringsarbetet för större övningar med många övade aktörer bör starta i mycket god tid – det kan handla om år i förväg. Förberedande planeringsmöten, för att förutsättningslöst diskutera övningsidéer och ambitionsnivå mellan uppdragsgivare/beställare och projektledning, hålls vanligen under fasen "övningsförberedelser". I samband med ett första möte är det lämpligt att forma organisationen för planeringen av övningen – alltså vilka aktörer som ska delta i planeringsprocessen och vilka roller de ska ha."[14]

Se figur 2 och 3 nedan för exempel på planeringsorganisationer för mindre och större informations- och cybersäkerhetsövningar.

Vid större tekniska informations- och cybersäkerhetsövningar bör även en *informationshanterings-/koordineringsansvarig*, samt ytterligare *ansvarig för media och kommunikation samt besökare* före, under och efter övningen utses. Dessa har till uppgift att samordna informationsflödet och se till att nödvändigt material från projektlednings- och övningsplaneringsprocessen finns tillgängligt för deltagarna i de medier som gemensamt beslutats om.

Media- och kommunikationsansvarig skriver och samordnar bland annat pressmeddelanden och inbjudningar till media och observatörer, handhar besöksprogram och sköter information till media och inbjudna i form av egna fördragningar eller koordinerar detta med andra tillgängliga för kommentarer under pågående övning.

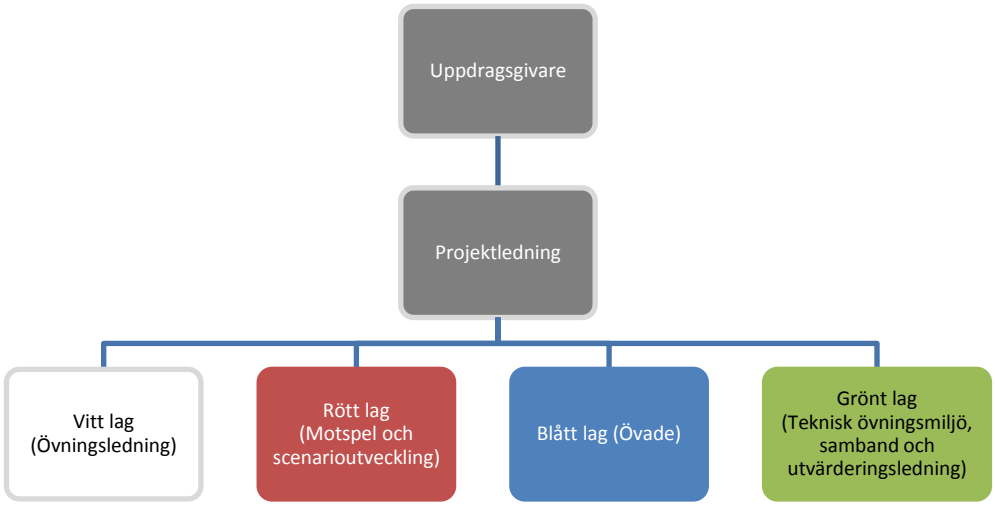
2.7.1 Arbetsgrupper och färger på arbetslagen

För informations- och cybersäkerhetsövningar av typen Rött lag/Blått lag används färgbeteckningar för arbetsgrupperna. Beteckningen *Rött lag* är för motspelsgruppen, tillika arbetsgruppen för scenarioutveckling om inte även Rött lag ska övas. För dessa fall och i större övningar brukar dock en separat arbetsgrupp utses för scenariot. Under övningen är det oftast *Blått lag* som övas. *Vitt lag* används för övningsledning och *Grönt lag* för arbetsgruppen för den tekniska övningsmiljön, teknik och samband.

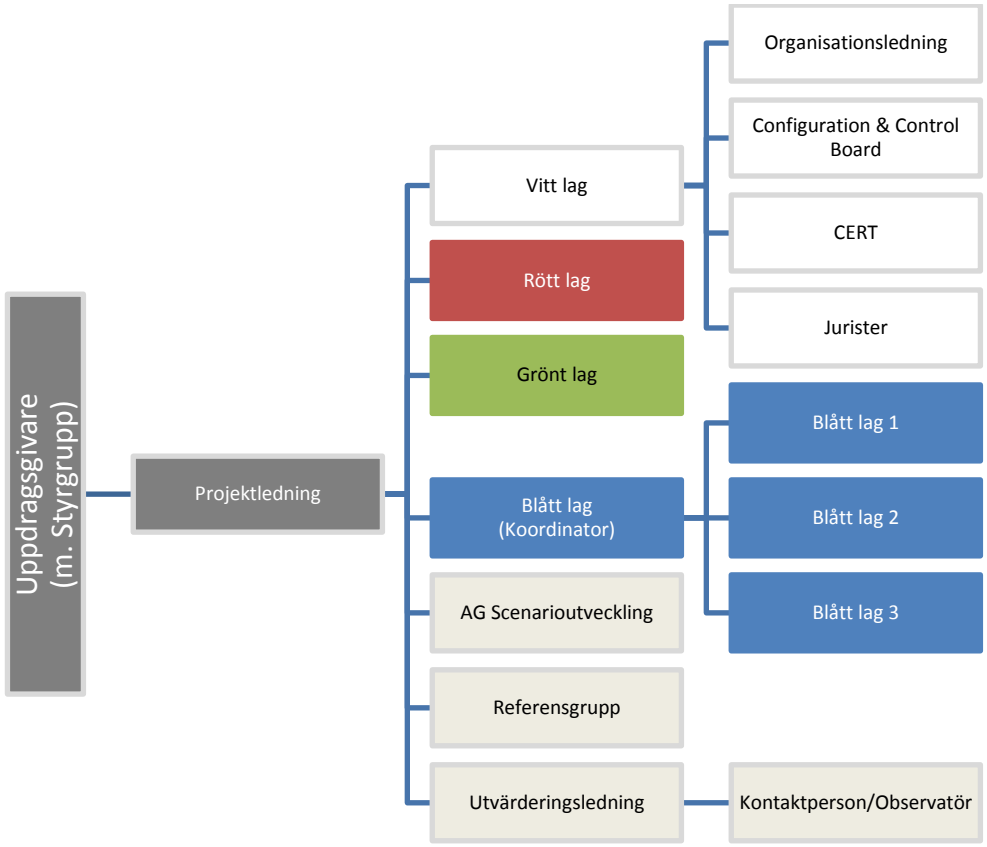
Ytterligare arbetsgrupper, till exempel för jurister (verksjurister, företagsjurister med flera), organisationens ledning och för utvärderingsgruppen, kan också tillkomma. Det är helt och hållet upp till projektledningen att bedöma och avgöra antalet arbetsgrupper och eventuella

[14] MSB (2009), s. 41.

färgbeteckningar.[15] Viktigt att beakta är emellertid att ju fler arbetsgrupper som finns, desto högre blir kraven på samordning, kommunikation och informationsdelning.



Figur 2. Ett exempel på en planeringsorganisation för mindre informations- och cybersäkerhetsövningar.



Figur 3. Ett exempel på en planeringsorganisation för större informations- och cybersäkerhetsövningar.

[15] Färgbeteckningen *Gult lag* har i övningsplanering använts för arbetsgruppen för scenarioutveckling. Det är även tänkbart att benämna den juridiska arbetsgruppen för *Lila lag*, arbetsgruppen för den övade organisationens ledning för *Orange lag* och till exempel utvärderingsgruppen för *Ljusgrönt lag*.

Tänk på att:

- övningens syfte, mål och målgrupp är avgörande för den fortsatta planeringen, genomförandet och återkopplingen. Sätt upp ”SMARTA” mål.
- inkludera såväl den tekniska ledningen för stöd och samband (ansvarig för infrastrukturen i informations- och cybersäkerhetsövningen) som utvärderingsledningen i övningsplaneringen *och* definitionen av syfte och mål.
- välja övningsmetod – övningsform och övningstyp – utifrån syfte och mål med övningen.
  För tekniska informations- och cybersäkerhetsövningar är ofta övningstypen *Red Team/Blue Team Exercise* (Rött lag/Blått lag-övning) att föredra då den lämpar sig för samtliga övningsformer (seminarium, simulering och skarpa övningar) och kan stödja olika målsättningar med övningen. Det är dock alltid syftet och målet med övningen som ska avgöra metoden för genomförandet.
- fastställa övningstider för när övningen ska hållas såväl som tider för övningens längd då detta har betydelse för scenarioutvecklingen för tekniska informations- och cybersäkerhetsövningen i nästa steg – praktiska förberedelser.
- sätta upp en planeringsorganisation med tydliga ansvarsområden för att underlätta samordningen med övningen och dess genomförande. Om möjligt samordna planeringsorganisationen (främst projektledning, övningsledning och motspelsorganisation/spelledning) fysiskt för att underlätta informations- och kommunikationshantering inom planeringsorganisationen.
- samordna informations- och kommunikationsdelningen – om möjligt till endast en plats för arkivering, dokumentation etcetera (men med möjlighet för otaliga kommunikationskanaler) – för en gemensam lägesbild.

3. Genomförande

Nedan ges en översikt av kriterier för den tekniska övningsmiljön i simulerade och skarpa informations- och cybersäkerhetsövningar samt tekniskt stöd och samband för dessa.

Läsanvisning
MSBs övningshandbok Del IV

3.1 Genomförandeorganisation

"Alla spel och övningar kräver en övningsorganisation av något slag för att kunna fungera vid själva genomförandet. Kraven på en sådan organisation ökar naturligtvis med övningens omfattning och komplexitet. Den allra enklaste organisationen vid små simuleringar eller spel kan vara att man inom övningsledningen enkelt kommer överens om vem som gör vad. Vid större övningar kan det krävas en organisation på 30 till 40 personer. Vilka aktörer och roller som kan finnas i övningsorganisationen framgår nedan. Beroende på övningens inriktning och omfattning kan vissa funktioner många gånger sammanföras eller organiseras på annat sätt."[16]

- Övningsansvarig – ansvarig för helheten
- Övningsledning – ansvarig för att målen uppfylls
- Övningsledare – ansvarig för genomförandet
- Spelledare – ansvarig för att spelet går som planerat
- Kontaktperson/observatör – ämnesexpert som dokumenterar
- Lokal övningsledare – ansvarig för lokal övningsledning
- Medie- och kommunikationsansvarig samt ansvarig för besöksprogram

3.1.1 Övningsdokumentation

Användbara dokument vid informations- och cybersäkerhetsövningar är förutom allmänna projektdokument även:

- övningsbestämmelser
- övningsledningsbestämmelser
- säkerhetsbestämmelser
- sekretessbestämmelser
- sambandsbestämmelser
- kontaktlista för övningsorganisationen
- utvärderingsdokumentation
- utvärderingsrapport av övade
- utvärderingsrapport av övningsprojektet

3.1.2 Scenario

"Med scenario menas en beskrivning av en tänkt förhistoria i en bestämd miljö och vid en bestämd tidpunkt, som leder fram till ett hot om en händelse eller en inträffad händelse. Hotet eller händelsen utvecklas så att vissa omedelbara konsekvenser uppstår följda av en viss konsekvensutveckling.
Scenariot kan delas in i:

- fasta förutsättningar
- förhistoria (tidigare händelseutveckling)
- startläge

[16] MSB (2009), s. 43.

- händelseförlopp
- omedelbara konsekvenser
- utveckling av konsekvenserna
- spelplan
- tekniskt bakgrundsmaterial."[17]

3.1.3 Spelmiljön

Den tekniska övningsmiljön (spelmiljön) för tekniska informations- och cybersäkerhetsövningar kan vara mer eller mindre omfattande beroende på syftet med övningen och vilken metod (övningsform och övningstyp) som valts.

För seminarieövningar kan det räcka med att presentationer och demonstrationer görs från en enskild dator utan nätverkskoppling, medan såväl simulerade som skarpa övningar förutsätter nätverk av sammankopplade datorer. Skarpa övningar sker även i existerande nätverk och i realtid medan den tekniska infrastrukturen är fiktiv för simulerade övningar.

Spelmiljön kan byggas av en enskild organisation för dess egna övningar eller till exempel hyras eller köpas in från en extern leverantör. För offentliga myndigheter gäller i dessa sammanhang Lag (2009:1091) om offentlig upphandling enligt nedan.

3.1.4 Upphandling

Vid upphandlingar av teknisk infrastruktur för informations- och cybersäkerhetsövningar bör bland annat följande beaktas.
Upphandlande myndigheter ska följa gällande lag (2009:1091) om offentlig upphandling för offentliga myndigheter vilken eftersträvar upphandling i konkurrens. Inom den offentliga sektorn kan upphandling även ske mellan statliga myndigheter och verk. Det ska dock alltid eftersträvas med en affärsmässigt sund kund- och leverantörsrelation. Upphandlingen bör delas upp i olika delar beroende på den beställda tjänsten eller varan. Ett exempel på uppdelning kan vara:

- teknisk infrastruktur respektive
- service (support) av teknisk infrastruktur.

Den tekniska infrastrukturen (spelmiljön eller övningsnätverket) består av teknisk utrustning såsom nätverksutrustning, servrar, datorklienter, programvara, videokonferensutrustning med mera. Infrastrukturen är relativt statisk och ger möjlighet för upphandling till fast pris.

Vid planering och genomförande av övning krävs även service (support) av den tekniska infrastrukturen. Det är svårt att på förhand planera för detta resursbehov vilket gör det svårt att upphandla till fast pris. Notera emellertid att den grundläggande supporten avseende de delar som är specificerade i den tekniska infrastrukturen också ska vara inkluderade i upphandlingen av den tekniska infrastrukturen.

3.2 Simuleringsövningar

3.2.1 Bakgrund

Följande avsnitt är baserat på praktiska erfarenheter från tidigare genomförda tekniska informations- och cybersäkerhetsövningar. Bland dessa är de tre simulerade och distribuerade övningarna CDX-I, II och III, seminarieövningen Nationell informationssäkerhetsövning (NISÖ) 2010, samt en informationssäkerhetsövning i skarpa system genomförd några år tidigare.

[17] MSB (2009), s. 54.

Avsnittet är inte allomfattande eller avser ge en uttömmande bild av hur tekniska informations- och cybersäkerhetsövningar kan eller ska planeras, genomföras eller återkopplas, utan presenterar utifrån tidigare ovan nämnda övningar rekommendationer och förslag till hur tekniska övningar kan se ut och vad som mer specifikt bör beaktas.

Övningsformerna kompletterar varandra och en övning kan ha inslag av olika former om detta är lämpligt för att uppnå övningens syfte och mål.
För tekniska informations- och cybersäkerhetsövningar används ofta en specifik övningstyp benämnd *Red Team/Blue Team Exercise* (Rött lag/Blått lag-övning). Samtidigt som den är en egen typ av övning kan den även omfatta andra övningstyper (larmövning, startövning, stabsövning, beslutsövning, ledningsövning, samverkansövning). Det vill säga att en Rött lag/Blått lag-övning exempelvis kan syfta till att öva såväl stabsarbete och beslutsfattande som samverkan i samma övning. Detta gör den till en ”flertypsövning”.

3.2.2 Mindre simuleringsövning med motspel

Simuleringsövningar kan genomföras i form av mindre övningar där bara en eller ett fåtal tjänster, till exempel ett DMZ, sätts upp och där endast en blå och en röd sida deltar.[18] En mindre övning kan utformas för att belysa specifik problematik som exempelvis hur attacker sker mot webbtjänster och hur dessa kan upptäckas.

Även om det är frågan om övningsverksamhet av mindre omfattning kan tillämpliga delar av övningshandboken nyttjas. Det är dock viktigt att alltid först fastställa syftet och målet/målen med övningen. Den teknik som används för övningsmiljön ska därefter väljas i enlighet med dessa för att även att i efterhand och genom utvärderingen utvisa hur väl dessa uppnåtts.

Tekniken i det simulerade övningsnätverket/övningsmiljön kan utgöras av enstaka datorer som återspeglar en verklig miljö. Det kan till exempel vara en kopia av en webbserver, brandvägg eller liknande som implementeras i en avskild miljö. Utvärdering kan genomföras kontinuerligt genom att:

- Rött lag genomför en eller flera olika attacker.
- Blått lag analyserar och rapporterar vad som sker.
- Övningen bryts och Rött och Blått lag går gemensamt igenom vad som har skett och vad som har upptäckts.
- Övningen fortsätter.

3.2.3 Större simuleringsövning med motspel

Övning i simulerad miljö ställer andra krav på genomförandet än i skarp ledningsmiljö. Deltagarna genomför övningen skild från den ordinarie verksamheten.

Rekommendationerna nedan utgår fram för allt från identifierade lärdomar av Baltic Cyber Shield 2010 (CDXII)[19]. Övningen var av typen Rött lag/Blått lag-övning med fördefinierade färgbeteckningar för arbetsgrupperna. Beteckningen *Rött lag* användes för motspelsgruppen som under övningen utsatte informationssystemen hos övade *Blå lag* för attacker och intrång. *Vitt lag* användes för övningsledning och *Grönt lag* för arbetsgruppen för den

[18] DMZ står för *demilitariserad zon*.
[19] För en utförlig beskrivning av övningen, dess organisation, scenario och genomförande hänvisas till den offentliga rapporten från övningen Baltic Cyber Shield Cyber Defence Exercise 2010, After Action Report. For Public Use. Tillgänglig via: https://www.fhs.se/sv/forskning/centrumbildningar-och-forskningsprogram/cats/nyheter-och-artiklar/2010/ (publicerad 2010-10-06).

tekniska övningsmiljön, teknik och samband samt datainsamling för utvärdering och analys.

3.2.4 Ansvarsfördelning

Målen för övningen ska fastställas under övningsplaneringen för att vara tydliggjorda innan de praktiska förberedelserna och planeringen för den tekniska miljön/infrastrukturen börjar. Om målet med övningen till exempel är att öka kunskapen om generiska attacktekniker och tillämpliga skyddsåtgärder, är kravet på den simulerade miljön lägre än vid övningar som ska efterlikna den övade organisationens verkliga (skarpa) system. I båda fallen krävs dock långtgående planerings- och testverksamhet av fram för allt Rött lag (motspelsgruppen) samt därtill god koordinering med Grönt lag (arbetsgruppen för den tekniska övningsmiljön, teknik och samband) och Vitt lag (övningsledningen).

3.2.5 Rött lag – Motspelsgruppen

Rött lag ansvarar för att de sårbarheter som finns, alternativt inplanteras, i den simulerade miljön kan exploateras på ett sådant sätt att de inte menligt påverkar simuleringsmiljön negativt ur ett övningstekniskt perspektiv. Exempelvis kan en sårbarhet åstadkomma bortfall av hela miljön som gör att övningen måste startas om. Rött lag ska för de planerade åtgärderna kunna redogöra för Blått/Blå lags möjligheter att upptäcka dessa.

3.2.6 Grönt lag – Arbetsgruppen

Grönt lag ansvarar för den simulerade miljön. Ett nära samarbete mellan Rött lag och Vitt lag måste ske under hela planeringsprocessen. Vid flera Blå lag som övas ska det eftersträvas att de har samma simulerade miljö. Denna miljö bör om möjligt kunna återskapas med kort varsel.

3.2.7 Vitt lag – Övningsledning

Vitt lag ansvarar för planläggning av scenariot för övningen. Detta görs med fördel av separat arbetsgrupp knuten till det vita laget. Samarbete med framförallt Rött lag måste ske i planeringen av olika övningsmoment. Vitt lag ansvarar även för den dokumentation (övningsbestämmelser, övningsledningsbestämmelser, säkerhetsbestämmelser, sekretessbestämmelser och sambandsbestämmelser samt kontaktlista) som ska delges övningsdeltagarna inför övningen. Utvärderingsdokumentationen bör sammanställas av utvärderingsgruppen parallellt med övrig dokumentation och likt denna delges deltagarna i god tid före övningen.

3.3 Teknik under planerings- och genomförandefaserna

3.3.1 Övningsnätverk

Övningsnätverket kan vara centraliserat och/eller distribuerat. Vid båda typerna förutsätts att övningsnätverket är separerat från andra nätverk med godkända mekanismer. För ett distribuerat nätverk kan detta utgöras av godkända krypterade tunnlar och för ett centraliserat nätverk av fysisk separation. Regler för anslutning av utrustning i ändpunkterna i ett distribuerat nätverk måste klarläggas för att inte få oönskade kopplingar i övningen till andra nätverk.

När behov finns för uppkoppling mot externt nätverk, till exempel för att hämta uppdateringar från Internet ska om möjligt detta göras med en kontrollerbar flyttning av information med till exempel USB-minne. Om en galvanisk koppling krävs måste detta utgöras av godkänd mekanism, till exempel brandvägg med *proxy*-funktionalitet. För varje typ av koppling mot ett externt nätverk ska en risk- och sårbarhets-/konsekvensanalys genomföras. Övervakad kopplingspunkt bör vara centralt placerad för hela nätverket.

3.3.2 Klientutrustning för Blått lag

Utrustning för Blått lag bör specificeras så att alla lag, om flera blå lag deltar, ges lika förutsättningar i övningen. Vid användning av krypterade tunnlar ska om möjligt utrustning för detta distribueras i god tid före övningen för att möjliggöra testning av övningsnätverket. Detta bör sammanhållas av Grönt lag (ansvarigt för teknik och samband).

3.3.3 Simuleringsmiljön

Den miljö som övningen bedrivs i kan med fördel utgöras av virtuella system. I en virtuell miljö finns ofta möjligheter till ögonblicksbilder (så kallade *snapshots)* som kan utgöra ett sparat gemensamt läge som kan återskapas på kort tid. Övningen kan därmed startas om från ett givet läge under övningen. Utmaningen för den simulerade miljön är så långt som möjligt kunna återspegla den verkliga miljön som Blått/Blå lag känner sig förtroget/-na med för att erhålla en realistisk övning.

De tjänster som ska vara implementerade bör utgöras av tjänster som är likadana dem som finns i ett skarpt nätverk.
För Rött lag (motspelsorganisationen/antagonisterna) utgör simuleringsmiljön den plattform som det ska implementera sårbarheter i. Sårbarheter bör utgöra realistiska hot som även är möjliga i en skarp miljö. Dessa sårbarheter ska testas så att de ger det resultat som kan förväntas.

3.3.4 Uppföljning

Rutiner för att följa upp incidenter (åtgärder/attacker) måste planeras och testas om de är beroende av tekniska system. Till exempel om ett felrapporteringssystem används i den normala driften bör ett liknande system ingå i övningen.

För varje åtgärd som Rött lag gör i den simulerade miljön ska det finnas planerade rutiner för hur man följer upp dessa, vad det förväntade utfallet är av åtgärden, vad som förväntas av Blått lag och eventuell poängsättning för Blått lag. Hänsyn måste tas till om en åtgärd påverkar annat än det specifika övningsmomentet. Till exempel kan en attack mot DNS även slå ut rapporteringsvägar och åtkomst till system som övningstekniskt krävs för en fungerande övning.

3.3.5 Poängsättning

En övning kan genomföras med eller utan poängsättning. Motivationen bland de övade höjs emellertid oftast om övningen samtidigt utformats med poäng för försvar (Blått lag).
En viktig del av den löpande uppföljningen under genomförandet av övningen är således poängsättningen. Övningens mål styr vad som ska prioriteras i bedömningen. Vitt lag som ansvarar för poängsättningen under genomförandet bör erhålla stöd av ett automatiserat system så långt som möjligt. Uppföljning av till exempel tillgängligheten till tjänster kräver stora personella resurser om flera Blå lag ska kunna bedömas likvärdigt.
Mål för poängsättning kan vara:

- tillgänglighetsmål
- integritetsmål
- sekretessmål.

Nedan följer exempel på automatiserade system för poängsättning av dessa mål.

Tillgänglighetsmål. I övningens mål kan exempelvis upprätthållande av interna och externa tjänster vara uppsatta. Dessa tjänster kan oftast kontrolleras med program som automatiskt kan känna av om de är aktiva eller inte. Exempel på dessa tjänster är: Webb, e-post, FTP, databas etc.

Integritetsmål. Uppföljning av integritet kan ske genom att automatiskt kontrollera om förändringar skett av filer i systemet.

Sekretessmål. Detta kan indirekt mätas som integritetsmål. En förändring av Rött lag av en ”hemlig” fil kan i de flesta fall anses vara tillräckligt för att bevisa förlust av sekretess.

3.4 Informations- och kommunikationssystemlösningar

Vid planeringens början under de praktiska förberedelserna bör en informations- och kommunikationsmodell utvecklas. De tekniker som används för planeringen kan skilja sig åt från dem som används under övningsgenomförandet.

3.4.1 Kommunikation

Vid övning i simulerad miljö finns två typer av kommunikation:

- intern kommunikation och
- extern kommunikation.

Intern kommunikation är all den kommunikation som sker internt i övningsnätverket. Detta kan vara krypterade tunnlar mellan den simulerade miljön/infrastrukturen och de olika lagen, informationsutbytestjänster i övningsnätverket som till exempel e-post, chatt, Voice over IP (VoIP) etc.

Extern kommunikation är den kommunikation som sker utanför övningsnätverket som till exempel ordinarie e-post, telefoni, chatt etc. Lämpligheten i vad som ska väljas för varje övning ska med fördel beslutas i planeringsfasen, eller senast under de praktiska förberedelserna. Vid intern kommunikation är kommunikationen vanligen skyddad mot extern exponering, men medför att beroendet av övningsnätverkets tillgänglighet ökar. Vid extern kommunikation kan man få en ökad tillgänglighet som inte beror på övningsnätverkets tillgänglighet, men medför också en större exponering av pågående verksamhet.

3.4.2 Allmänna råd

- Minimera det antal ställen som information finns lagrad på.
  - Att kombinera både *peer-2-peer*-nätverk som exempelvis Groove med ett centraliserat system som Wiki eller Sharepoint medför onödig risk för inkonsekvens i informationen.
  - Versionshantering av information bör ske med stöd av mjukvara. Exempelvis kan subversion eller motsvarande utgöra grunden för att lagra information.

- Välj om möjligt lösningar som är plattformsoberoende.
  - Beroendet av speciell teknologi eller speciella program bör undvikas. Användare bör kunna använda de system som man normalt sett är familjära med. De lösningar som bör väljas bör kunna fungera i Microsoft Windows, Linux, MacOS etc.

- Genomför utbildning på vald kommunikationslösning och informationsstrategi.
  - I uppstarten av övningsprojektet (under de praktiska förberedelserna) bör hjälp och utbildning finnas för de lösningar som valts. Denna bör omfatta hur man arbetar med information, versionshantering, klassning, spridning, mallar, namnsättning, kvalitetssäkring, fastställande etc.

- Sekretess.
  - Vid val av informations- och kommunikationslösning(ar) ska ett behovsanpassat sekretesskydd tillgodoses.

3.4.3 Informations- och kommunikationslösningar under genomförandet av övningen

De allmänna råden i ovan gäller även under övningens genomförande, utvärdering och för återkoppling.

Det som tillkommer under genomförandet är att informations- och kommunikationslösningarna kräver mer tillgänglighet av både teknik och personal. Informationsutbyte mellan de deltagande lagen kan här ske både inom och utom övningsnätverket. Båda sätten ska vara planerade för att möjliggöra redundans.

Informationsutbytet mellan Vitt lag och Blått lag ska i första hand utgöras av e-post och om möjligt av ett *"ticket*-system". Detta är ett rapporteringssystem där mallar för rapportering är fastställda. Åtkomst bör möjliggöras både inom och utom övningsnätverket.

För att underlätta informationsutbyte mellan övriga enheter i övningsledningen bör samgruppering eftersträvas. Kan inte detta ske bör videokonferens med möjlighet till presentation samt flerpartskonferens, om enheterna är spridda på mer än en plats, utnyttjas. Även om övningsledningen är samgrupperad kan videkonferens vara användbart mellan de olika lagen.

Att tänka på vid val av informations- och kommunikationslösning under genomförandet

- Vad måste sparas för att kunna utvärdera övningen?
  - Olika lösningar ger olika möjligheter till att spara information för utvärdering och uppföljning. Textbaserad information, till exempel e-post, "*ticket*-system", elektroniska dokument med mera är enklare att spara än mer realtidsnära kommunikation som telefoni.

- Tidssättning.
  - Gemensam tidskälla bör användas av all teknisk utrustning för att underlätta samstämmighet av olika informationskällor. Denna tidskälla kan med fördel utnyttjas med NTP (*Network Time Protocol*). Det är inte kritiskt att det är absolut rätt tid utan att alla har samma tid.

- Minimera antal system där information lagras på.
  - För att undvika inkonsekvens i informationsutbyte och lagring bör strävan vara att informationen endast finns på en plats (eller två om man räknar med ’backupen’ som naturligtvis ska finnas med).

3.5 Styrning av övning

3.5.1 Övningsledning

Vitt lag (övningsledningen) ska delta i planeringen av Rött lags (motspelets) åtgärder med fram för allt vilka medel som krävs för att följa upp Blått lags (de övades) åtgärder. I denna planering sätts även reglerna för eventuell poängsättning.

Vitt lag ansvarar för att nödvändiga rapporteringsverktyg finns för Blått lag. En begränsning av antal rapporteringsvägar underlättar koordineringen i Vitt lag. Om möjligt bör, enligt ovan, ett ”ticket-system” utnyttjas, (till exempel OTRS)[20]. Anpassning av till exempel OTRS eller motsvarande bör ske i god tid före övningen. Därtill bör utbildning genomföras med deltagare för såväl Vitt lag som övade Blå lag. Det kan även finnas behov av att Rött lag ska rapportera i samma system.

Övningsledningens samordning mellan de olika lagen, Vitt lag (till exempel CCB och CERT), Rött lag, Grönt lag och Blått lag är under genomförande av stor vikt för att få ett bra flyt i övningen och hålla en god struktur under genomförandet.

En god lägesuppfattning krävs för att Vitt lag och Grönt lag ska kunna lösa sina uppgifter.[21] Under de praktiska förberedelserna bör man fundera kring hur detta kan skapas och under övningen delas mellan lagen. En gemensam lägesuppfattning är fram för allt nödvändigt för att Vitt lag ska kunna leda övningen och genomföra en rättvis poängsättning, samt för att Grönt lag ska kunna fatta nödvändiga beslut. Den är även användbar vid information till besökare under övningen. Delar av denna lägesuppfattning behöver även kontinuerligt kommuniceras till de blå lagens observatörer. Lägesbilden kan enkelt åskådliggöras i en uppföljningsmatris med delmål där resultaten anges för vart och ett av de övade lagen.

3.5.2 Planering av motspelsorganisationen - Rött lag

Planeringen för genomförande av motspelsorganisationens aktiviteter är beroende av flera faktorer. Några exempel på dessa är:

- målen med övningen
- övningsdeltagarnas kunnande och utrustning
- övningsnätverkets uppbyggnad
- styrning och uppföljning

3.5.3 Överensstämmelse mellan mål och övningens upplägg i faser

De aktiviteter som Rött lag (motspelet) genomför i övningen ska ha en spårbarhet till målen med övningen. Målen kan lämpligen brytas ned till att överensstämma med olika faser där starten av varje fas styrs av det Vita laget (övningsledningen).
Ett exempel på detta är hur Blått lags (övades) övningssystem kan vara uppbyggt av tre delar:

- DMZ

---

[20] Se vidare om *Open Technology Real Services* via http://www.otrs.org
[21] Enligt proposition 2007/08: 92, Stärkt krisberedskap – för säkerhets skull, definieras *lägesuppfattning* som ”en bedömning av hur det som inträffat påverkar aktörens sammanhang. Lägesuppfattningar bygger således på en lägesbild. Både lägesbild och lägesuppfattning är kopplade till beslutsprocesser och behövs som underlag för att kunna avgöra om agerande krävs på något sätt och i så fall hur”.

  - DMZ är den zon som publika tjänster normalt placeras i. Det är denna del som är ansluten mot Internet.

- INTERNAL
  - Detta är det ordinarie kontorsnätet som bara ska vara tillgängligt för behörig personal.

- SCADA
  - Industrisystem med både processtyrningsutrustning och användargränssnitt.

Övningen kan exempelvis delas in i tre faser där DMZ, INTERNAL och SCADA är fokus i varje fas.

3.5.4 Tekniska rapporteringssystem

För tekniska informations- och cybersäkerhetsövningar kan tekniska rapporteringssystem byggas in i den simulerade övningsmiljön samtidigt som existerande system kan användas/testas under en skarp övning. Här är övningens syfte och mål styrande för hur utvecklade dessa bör vara för att fungera under övningen och för att kunna bidra till utvärderingen av övningen under dess genomförande. Ett rapporteringssystem kan till exempel vara relativt enkelt och bestå av ett e-postsystem som antingen integrerats i övningens infrastruktur eller finns utom denna.

Samtidigt som ett tekniskt spelstödssystem kan vara behjälpligt för övningsledningen och motspelsorganisationen under övningen kan det likt beskrivningen ovan även tjäna som underlag till utvärderingen av övningen. Det kan även sammanlänkas med en teknisk lägesbildsfunktion (programvara) som dels visar var i övningen lagen befinner sig, dels om och hur de har reagerat på tidigare inspel och vilka inspel som kommer. En teknisk/datoriserad visuell lägesbildsfunktion kan användas för både spelledning och motspelsorganisation, likväl som för besökare till övningen.

3.6 Skarpa övningar

Denna typ av övning lämpar sig för att öva beredskap och hur väl till exempel incidenthanterings- och rapporteringsverksamheten fungerar. Denna övningsform ställer dock stora krav på övningens genomförande så att inte driftsäkerheten i det skarpa (verkliga) systemet påverkas. Övningsformen kräver att risk- och konsekvensanalyser görs såväl innan övningen som under dess genomförande. Detta på grund av att inga svagheter på förhand kan inplanteras i de övade systemen. Konsekvenser för hur funna svagheter ska utnyttjas under övningen behöver bedömas utifrån deras påverkan på verksamheten som helhet. Personer med stor kunskap om verksamheten som övas (till exempel säkerhetschef och verksamhetschefer) ska ingå i övningsledningen för att delta i bedömning av huruvida till exempel en viss server får stängas ned eller inte.

Information om övningens genomförande har normalt sett en begränsad spridning. Övad organisation genomför detta i ordinarie verksamhet.

3.6.1 Planering

Vid planering av övningar i organisationens skarpa miljö ska två grupper delta: Vitt lag (övningsledning) som även består av en säkerhetschef (eller motsvarande) från den övade organisationen med god kunskap om den tekniska infrastrukturen (IT, nätverk etc.) och dess ledningssystem, samt rött lag som utgör antagonistaktören (motspelsorganisationen). God kunskap om

vad som kan påverka ledningssystemet negativt krävs för att före övningen kunna genomföra en riskanalys. Rött lag måste här kunna göra en konsekvensanalys av *alla* planerade åtgärder (attacker).

Underlag för det röda laget (motspelsorganisationen) kan utgöras av information om informationssystem och nätverken, nätverksdiagram, ledningssystemkomponenter, versioner av operativsystemen, applikationsinformation etc.

3.6.2 Attackvägar

Vid genomförandet av en övning i skarp miljö måste man ta hänsyn till exponeringen av åtgärder (används omväxlingsvis med attacker) från Rött lag (motspelsorganisationen). Åtgärder som genomförs från den övade organisationens icke-kontrollerbara nätverk bör om möjligt undvikas för att minska eventuell exponering av sårbarheter.

3.6.3 Genomförande

Vid genomförandet får endast attacker som under de praktiska förberedelserna godkänts av Vitt lag (övningsledning) genomföras. För uppkomna åtgärder som inte kunnat planläggas under förberedelserna till övningen, måste en konsekvensanalys och riskbedömning genomföras och godkännas av Vitt lag före det att åtgärden aktiveras.

3.6.4 Kommunikation

Ordinarie vägar för intern rapportering används för kommunikation av den övade organisationen (ett eller flera Blå lag). Vitt lag och Rött lag (d.v.s. övningsledning och spelledning med motspelsorganisation) bör sitta samlokaliserade för att underlätta kommunikationen inom övningen. Den övade organisationen kan till exempel ha medlemmar från ledningsgrupp, kommunikatörer och en eller flera jurister med i motspelet vilka under övningen deltar utifrån sina ordinarie befattningar och utgör del av den ordinarie rapporteringskedjan.

3.6.5 Uppföljning

Vid planeringen ska man beakta vad som förväntas av den övade organisationen och hur detta kan kontrolleras för uppföljning under återkopplingen av övningen. Rapportering sker i ordinarie rapporteringssystem. Ett planerat uppföljningsmöte med Blått lag, Vitt lag och Rött lag (d.v.s. övade, övningsledning och spelledning med motspelsorganisation) bör ske under slutfasen av övningen där en genomgång görs av vad som tekniskt skett i systemen. Detta omfattar vilka åtgärder Rött lag genomfört samt vad detta medfört i den övade organisationen av Vitt lags deltagare (övningsledning och deltagare från den övade organisationen på till exempel ledningsnivå). Under detta uppföljningsmöte bör lämpliga åtgärder att implementeras av den övade organisationen diskuteras.

Tänk på att:

- sätta upp en övningsorganisation för genomförande av övningen som möjliggör fysisk samordning av övningsledning och motspelsorganisation/spelledning.
- övning i simulerad miljö ställer andra krav på genomförandet än i skarp ledningsmiljö. Deltagarna genomför övningen skild från den ordinarie verksamheten.
- minimera det antal ställen som information finns lagrad på.
- välj om möjligt lösningar som är plattformsoberoende.
- informera vid genomgångar övningens samtliga deltagare om vald informations- och kommunikationslösning samt

kommunikationskanaler.

4. Utvärdering

Nedanstående avsnitt behandlar utvärdering av en övning. Den övergripande tanken med att utvärdera övningar är att skapa förutsättningar för att öka det individuella och organisatoriska lärandet.

Läsanvisning
MSBs övningshandbok Del V

4.1 Återkoppling och återrapportering

För tekniska informations- och cybersäkerhetsövningar kan en kombination av tekniska och manuella system för datainsamling och analys vara att föredra. Den tekniska datainsamlingen kan bestå av ljud och bild-upptagningar, datoriserade enkäter (via Internet-formulär) samt dataloggar. Systemet eller systemen för datainsamlingen kan antingen utvecklas inom den övade organisationen eller upphandlas av tredje part. Efter övningens genomförande kan insamlad data bidra till att återskapa övningen för mer detaljerad analys.

Den manuella datainsamlingen består ofta av direkta observationer från en eller flera observatörer som finns med i de deltagande lagen/arbetsgrupperna under övningen. Dessa observatörer kan både vara delaktiga i den tekniska datainsamlingen (hantera ljud- och bildupptagningar) och anteckna sina observationer av de deltagande lagen under övningen.

Observatören kan även bidra till att uppdatera övningsledningens och spelledningens lägesbild under genomförandet av övningen, då denne kan rapportera om hur inspel har mottagits och åtgärder vidtagits. I det fall tekniken skulle fallera kan observatören även bidra till lägesbild och material för utvärderingen genom personliga intervjuer med övningens deltagare.

4.1.1 Verktyg för utvärderingen

Utvärderingsarbetet bör pågå från planeringsfasen (genom att även utvärderingsorganisationen sätts upp parallellt med övriga arbetsgrupper) och genom hela övningen till dess avslut. Utvärdering av övningar bidrar till identifierade lärdomar som genom uppföljning kan integreras i arbetet med nya övningar.

Även om utvärderingsarbetet med övningar är relativt lika, skiljer sig möjligen tekniska informations- och cybersäkerhetsövningar något från mängden. Samtidigt som datainsamling enligt utvärdering av övningar kan ske på flera sätt, ger tekniska övningar bättre förutsättningar för att med hjälp av olika tekniska verktyg och system samla in data via enkäter till övningsdeltagarna som fylls i on-line, dataloggar från systemtrafiken i övningsnätverket m.m. samt inspelningar (ljud och bild) som komplement till observatörernas egna observationer av de övade lagen (Blått, Rött, Grönt, Vitt).

Det är dock såväl värdefullt som nödvändigt att under planeringen av övningen besluta vad utvärderingen ska fokusera på (kopplat till övningens syfte och mål) då såväl insamlingen av data som genomgången av denna efter övningen är resurskrävande i tid och kostnader för teknik och personal.

4.1.2 Utvärderingsprocessens steg

En utvärderingsprocess består av ett antal. För mer information om innehållet i varje steg nedan, se MSB:s *Handbok – Utvärdering av övningar*.[22]

1. Utse en utvärderingsledare
2. Planera och organisera utvärderingen i samverkan med övningsledningen
3. Formulera utvärderingsfrågor och underlag för analysen
4. Utbilda utvärderarna
5. Observera övningen och genomför en direktåterkoppling
6. Analysera insamlat material och sammanställ utvärderingsrapporten
7. Presentera och sprid utvärderingen
8. Ta tillvara lärdomar och börja planera nästa övningsinsats

4.1.3 Återkoppling

Återkopplingen av erfarenheter från övningen görs med fördel en kortare tid efter övningens avslut. Detta ger utvärderaren möjlighet att samla ihop erfarenheter från de övade efter den direkta erfarenhetsåterföringen efter övningen, samt från en första översikt av insamlat material från observationer av övningen. Återkopplingen kan ske genom ett återkopplingsseminarium där utvärderaren får presentera de första slutsatserna från övningen och diskutera och stämma av dessa med övningsdeltagarna inför färdigställandet av den slutliga övningsrapporten/utvärderingsrapporten efter övningen.

4.1.4 Återrapportering

När resultaten från övningen är analyserade och sammanställda görs en återrapportering till beställaren. Dels kan det vara resultat och erfarenheter av det som övades under övningen, dels kan det vara erfarenheter av själva övningsprocessen och valet av övningsform etc.[23]

Återrapporteringen är en fortsättning på inventering och behov av övning som tidigare delmoment under övningsförberedelser i planeringen

Tänk på att:

- övningens syfte och mål avgör vilken data (*vad*) som ska samlas in. Besluta först därefter om datainsamlingsmetod (*hur*) – teknisk och eller manuell datainsamling – och informera övningsdeltagarna om detta.
- hålla en enklare återkoppling, s.k. *hot wash*, med övningens lagledare i direkt anslutning till den genomförda övningen för att fånga upp deltagarnas erfarenheter inför återrapporteringen och analysen för övningens utvärdering.
- när resultaten från övningen/projektet utvärderats och presenterats kan dessa efter uppföljning leda till nya utbildnings-/övningsinsatser, förslag till förändringar av organisation eller processer med mera.

[22] MSB (2010), *Handbok – Utvärdering av övningar*, Myndigheten för samhällsskydd och beredskap. (Tillgänglig via: https://www.msb.se/RibData/Filer/pdf/25490.pdf, 2012-06)
[23] MSB (2009), s. 89.

5. Erfarenheter från CDX-övningarna

5.1 CDX-I

IT-attackerna mot Estland var den händelse som initierade det internationella samarbetet och den övningsverksamhet som startade 2008. Totalförsvarets Forskningsinstitut (FOI) vidareutvecklade, på uppdrag av dåvarande Krisberedskapsmyndigheten (KBM), sitt befintliga IT-lab till att även omfatta säkerhet i SCADA-system och Försvarshögskolan (FHS) påbörjade uppbyggnaden av ett IT-lab. Dessa lab användes i den övning CDX-I, som genomfördes 12 juni 2008. Deltagare var FHS/ Centrum för asymmetriska hot- och terrorismstudier (CATS) , FOI, Försvarets radioanstalt (FRA), KBM, Försvarets materielverk (FMV) och Cooperative Cyber Defence Centre of Excellence (CCD COE) från Estland. Övningen syftade på att ta fram ett koncept för övning som bygger på ”Red Team”-metodologi.[24]

Eftersom övningen syftade till att lära sig att genomföra och planera IT-säkerhetsövningar utgick inte planeringen från någon framtagen metodik. Lärdomarna av övningen är framförallt att man inte ska underskatta komplexiteten av de tekniska komponenterna både i övningsnät och i ledningsnät. Till synes enkla komponenter kan bli komplexa i en internationell distribuerad offentlig/privat samverkan.

Utvärderingen av CDX-I pekade på behovet av att utveckla en metodik och kunskap om planering och genomförande av övningsformen. Under perioden tecknades ett samarbetsavtal mellan FHS och CCD COE som gav möjlighet till ett internationellt samarbete för fortsatt utveckling av övningsformen samt genomförande av övning.

5.2 CDX-II[25]

Hösten 2009 startade planeringen av Baltic Cyber Shield 2010 (”CDX-II”). Övningen genomfördes maj 2010. Huvudaktörerna för planering och genomförande var CCD COE från Estnisk sida och FHS och FOI på uppdrag av MSB från svensk sida. I övningen deltog sex Blå lag som hade i uppgift att försvara en relativt komplex IT-infrastruktur som även innehöll SCADA system. De Blå lagen kom från NATO, Lettland, Litauen och Sverige. Målen med övningen var:

1. Utökad förståelse för den internationella cybermiljön (inklusive legala aspekter) och nödvändigheten till samverkan
2. Utveckla samt utöka internationell samverkan inom förmågan att tekniskt hantera cyber incidenter
3. Utöka samverkan på myndighetsnivån (nationellt)
4. Utöka samverkan mellan offentlig och privat sektor

[24] Slutrapportering skedde till MSB i januari 2009, FHS beteckning 415/7:31.
[25] Avsnittet är ett utdrag från ”Rapport efter CCD COE – Swedish CDX 2010”, Mj J. Karlsson, intern rapport till MSB, Försvarshögskolan, Centrum för asymmetriska hot- och terrorismstudier, maj 2010.

5. Öva IT-säkerhetsstudenter samt yrkesverksamma inom området
6. Förbättra kompetensen avseende genomförandet av tekniska övningar
7. Studera attacker samt skydd av CII/SCADA
8. Utbyta information och erfarenheter

CDX-II var ett stort steg framåt för att utveckla förmågan att genomföra denna typ av övningar. Inför CDX-II avsattes mer resurser i planeringen än CDX-I. Den tekniska infrastrukturen utvecklades vidare och omfattande tester genomfördes av Grönt, Vitt och Rött lag före övningen.

Vitt lag - övningsledning
Vitt lag ansvarade under planeringen för att ta fram regler inklusive poängberäkning. Under genomförandet styrde Vitt lag tillsammans med spelledningen och motspelsorganisationen (Rött lag) övningen genom inspel från en förberedd spelplan (spelmeny). Vitt lag skötte den manuella poängbedömningen samt utvärderingen av de blå lagens insatser. Vitt lag ansvarade även för besökare och deras gästprogram.

Rött lag – motspelsorganisation
Rött lag hade till uppgift att kompromettera eller försämra funktionaliteten hos de system som de Blå lagen var satta att skydda. Detta skulle ske kontrollerat och med jämn effekt på lagen över tid. En preliminär fasindelning och målsättningstablå sammanställdes i förberedelseskedet för att skapa en god struktur på genomförandet.

Grönt lag – teknisk övningsmiljö
Grönt lag (gruppen för den tekniska övningsmiljön och teknik och samband), ansvarade för förberedelser av den tekniska infrastrukturen. Detta inkluderade VPN-tillgången till spelmiljön, skapandet av system för Blå lag, de olika presentationsareorna, loggningar med mera. Under genomförandet ansvarade Grönt lag även för rollen som Internet Service Provider (ISP) till de Blå lagen.

Blått lag - övade
Blått lag, som under övningen var flera, utgjorde de övade. Deras uppgift var att skydda den delvis förbyggda IT-infrastrukturen i en fiktiv organisation mot attacker från Rött lag.

5.3 CDX-III

CDX-2012/MNE7 ”Locked Shields” (”CDX-III”) genomfördes till större delen utan svensk medverkan. Det var i huvudsak ett samarbete mellan CCD COE i Estland, Finland och Schweiz. Den tekniska infrastrukturen byggdes av Schweiz (Grönt lag) utgående från erfarenheterna från CDX-II. På grund av att fler lag deltog i övningen ökade komplexiteten i infrastrukturen.

Organisationen för CDX-III bestod av nio Blå lag som spelade var sitt telekom företag som levererade ett antal tjänster till sina kunder. De hade målsättningen att upprätthålla dessa tjänster för att inte förlora poäng. Antagonisterna utgjordes av ett Rött lag som genomförde ett stort antal attacker mot de Blå lagen.

Det vita laget som ledde övningen och genomförde uppföljning var uppdelat i grupper om tre-fyra personer med olika ansvarsområden. Utöver vitt, blått och grönt lag, organiserat som i CDX-II, tillkom ett Legal Team som genomförde inspel av legala frågor, ett Gult lag som genomförde visualisering och analys av nätverkstrafik och ett Media-lag som spelade journalister och tog hand om besökare.

5.4 Jämförelse mellan de olika CDX-övningarna

5.4.1 Informationsutbyte

Planering av alla CDX övningar, genomfördes genom ett fåtal fysiska möten och övriga möten via videokonferens och telekonferens. Utbyte av information elektroniskt utvecklades från email under CDX-I till en mer renodlad dokumenthantering på en s.k. Wiki i CDX-III. Under CDX-II användes ett flertal dokumenthanteringssystem som t ex Groove och Wiki. Detta medförde emellertid svårigheter att veta vilken information som var giltig i alla lägen.

5.4.2 Scenario

Under de tre övningarna som genomförts har beroendet av ett välregisserat scenario inte varit så stort på grund av att fokus har legat på att lära sig att genomföra dessa övningar i en komplex miljö. De scenarion som dock förekommit har varit hantering av DDOS-attacker i CDX-I, skydd av infrastruktur i energibolag samt säkerställa tjänster inom telekom bolag (ISP) i CDX-III. I de båda sista övningarna har scenariot varit att de blå teamen fått uppgiften att ta över efter att ordinarie IT-avdelning antingen varit på konferens eller blivit avskedade.

5.4.3 Rött lag

Det har varit en betydande skillnad i resurser mellan de olika övningarna. Från ett fåtal deltagare i Rött lag i CDX-II till över 40 st. i CDX-III uppdelade i sex grupper specialiserade på olika teknikområden. I den senaste övningen spelade man även med två typer av attackerare, dels vanliga hackare som ville synas så mycket som möjligt och dels en grupp som försökte dölja sina attacker i största möjliga mån.

5.4.4 Vitt lag

Antalet deltagare i Vitt lag, har under genomförandefaserna ökat från ett fåtal till mer än 20 i CDX-III. Detta är inte enbart beroende av antal fler övade Blå lag (2-9) utan också på de erfarenheter som framförallt CDX-II gav. I Vitt lag under CDX-III fanns funktioner för incidenthantering med personal från CERT, kommunikatörer med de Blå lagen, personal som simulerade användare, support personal för kommunikationsinfrastruktur, de Blå systemen, automatisk poängberäkning, visualisering av nätverkstrafik samt även chef och ställföreträdare.

I CDX-III tog man också nytta av personal i Vitt lag för att genomföra attacker som kräver någon form av medverkan från användare i IT-systemet. Exempelvis kunde det vara att besöka websidor och ladda ner filer som innehöll skadlig kod.

Medias roll utvecklades i CDX-III till att dels omfatta spelade massmedia kontakter till de Blå lagen, och dels till att ta hand om besökare.

5.4.5 Grönt lag

Erfarenheterna från första övningen medförde en betydande tillväxt av den tekniska infrastrukturen till CDX-II. För CDX-III genomfördes utvecklingen av annan organisation och land men med erfarenheterna från CDX-II. Erfarenheten har visat att infrastrukturen i stort sett kan vara likadan oavsett vilket scenario som spelas. En betydande samverkan mellan Rött och Grönt lag måste ske under uppbyggnadsfasen för att säkerställa att attacker kan genomföras.

Grönt lag har även haft ansvar för kommunikation i genomförandet av övningarna. Ett stort antal chat-kanaler och epostkonton användes under CDX-II och CDX-III.

Automatisk poängberäkning användes som komplement till manuell bedömning. Den automatiska delen har byggt på att kontrollera om tjänster är aktiva i de Blå lagen. Den manuella delen utvecklades i CDX-III till att en etablerad CERT funktion bedömde incidentrapporter och hur de Blå lagen.

5.4.6 Legal Team

Legala aspekter och uppgifter till de Blå lagen utökades från CDX-II till CDX-III. Detta har skett med ett framtaget regelverk för övningen samt inspel av uppgifter att lösa.

5.4.7 Blått lag

Antalet Blå lag har gått från två till nio från den första till den senaste CDX-övningen. Den automatiska poängsättningen har i stort sett enbart kontrollerat att tjänster är aktiva i de Blå systemen och detta har medfört att prioritering av arbetet inom Blått lag blivit mer styrt av poängsättning än annat.

De Blå lagen har haft tillgång till övningsnätet före övningarna. Under CDX-III utgjordes dessutom första dagen av övningen av tester av hela den tekniska infrastrukturen så att alla lag var redo. Erfarenheter har visat att det krävs en dag som förövning.

6. Erfarenheter från NISÖ 2010 och Cyber Storm III

Nedanstående utgör en sammanställning av de erfarenheter som övningsledningen för *Nationell informationssäkerhetsövning 2010* (NISÖ 2010) och Cyber Storm III ansett vara särskilt viktiga att föra vidare i planeringsprocessen för NISÖ 2012.

1. **Utveckla området informations- och cybersäkerhetsövningar**
   - Det finns ett stort behov av övningar inom området – på alla nivåer i samhället. Det krävs dock stora resurser för att arrangera övningar, men även för att delta i övningar. Övningar måste därför utformas så att de ger deltagande organisationer nytta i sin dagliga verksamhet. Erfarenheter från övningar måste omsättas i praktiken.

   - För att skapa en bra mix av övningar behövs övningsprogram inom området. Samma typ av övningar passar inte i alla situationer. Nationella samverkansövningar behöver kompletteras med mer avgränsade, mindre, övningar. Övningar som fokuserar på policyaspekter behöver kompletteras med tekniska övningar och så vidare.

     I takt med att de nationella övningarna kan förväntas bli allt större i antal övade behövs en planeringscykel där aktörernas egna förberedelser utvecklas. Exempelvis kan en nationell övning föregås av mindre övningar i deltagande organisationer. Här kan centrala aktörer behöva ta fram metoder och material (exempelvis scenarier) som används i dessa förberedelser.

   - Övningar måste passas in i den ordinarie (löpande) verksamheten. Det behöver genomföras aktiviteter mellan övningar för att upprätthålla nätverk, kunskap etcetera.

   - Det är viktigt att fortsätta bygga upp förtroende mellan inblandade aktörer för att utveckla området.

   - Det finns ett fåtal nyckelpersoner inom informations- och cybersäkerhetsområdet. Av resurs- och kompetensskäl kan samma person både behöva delta i planeringen av en övning och i genomförandet.

   - Det är viktigt att samarbeta med andra länder kring informations- och cybersäkerhetsövningar. I detta bör ligga att delta i observatörsprogram och ordna besöksprogram vid egna övningar.

   - Metodiken för att planera, genomföra och utvärdera informations- och cybersäkerhetsövningar behöver utvecklas rent generellt. Detta gäller exempelvis hur scenarier och inspel konstrueras (se även punkt 3 nedan).

2. **Gå mer mot prövande informations- och cybersäkerhetsövningar**
   - Rutiner och arbetsformer inom området utvecklas ständigt så lärande övningar spelar fortfarande en viktig roll. Det är dock viktigt att öka de prövande inslagen och realismen (se punkt 3 nedan). Prövande inslag ”tydliggör och sätter problem på kartan”. Fler prövande inslag i övningar kan även vara ett sätt att driva utvecklingen av gemensamma

ramverk för samverkan samt processer och rutiner för hantering av allvarliga IT-incidenter.

- Vissa aktörsgrupper är redan idag mogna för prövade inslag. Olika aktörsgrupper kan ha olika grad av prövade element i en och samma övning.
- Oförberedda övningar, exempelvis larmövningar, bör genomföras i de grupperingar där etablerade ramverk och processer existerar.

3. Öka realismen i informations- och cybersäkerhetsövningar

- Involvera fler sektorer och kritiska beroenden, exempelvis elektroniska kommunikationer.
- Involvera fler organisationer i övningarna.
- Involvera fler roller som är engagerade i hanteringen av allvarliga IT-incidenter, exempelvis jurister.
- Att öka övningens storlek och komplexitet behöver inte göra den mer realistisk – en mindre och anpassad övning kan vara ett sätt att öka realismen för en given aktör (se även punkt 1 ovan).
- Olika aktörsgrupper måste övas utifrån sina förutsättningar för att öka realismen. Detta kan betyda att alla aktörer inte deltar samtidigt och att övningen genomförs utsträckt över tid.
- Den internationella dimensionen bör finnas med tydligare i övningarna. Exempelvis kan detta ske genom att engagera utländska ledningsfunktioner, specialister och leverantörer.
- Gör det möjligt för övningsdeltagarna att i högre grad öva i sina befintliga roller – öva exempelvis ordinarie krisledningsfunktioner (detta kan ske även om övningen inte är prövande.).
- Öka inslagen av distribuerade moment även i samverkansövningar.
- Informations- och cybersäkerhetsövningar ställer mycket höga krav på scenarier och inspel för att skapa realism. För vissa målgrupper behövs verklighetsnära scenarier och djupt tekniska inspel. Det är därför viktigt att i god tid innan övningen skapa ramscenarier som först kvalitetssäkras och sedan kan utvecklas till tekniska inspel av specialister. I vissa fall kan även verkliga händelser (analyserade och dokumenterade) användas som scenariounderlag eller inspel.

4. Några förslag på moment som kan behöva övas ytterligare i informations- och cybersäkerhetsövningar:

- Att skapa/upprätthålla lägesbilder och göra konsekvensbedömningar, exempelvis utifrån perspektivet samverkan mellan policy och teknik.
- Att skapa förutsättningar för aktörer att samordna budskap (kriskommunikation).
- Att återställa verksamheter och IT-system efter en allvarlig IT-incident.
- Att hantera incidenter som både beror på antagonister och olyckor – skillnader i operativa aspekter och policy/lagstiftning.

7. Praktiska råd och tips

Handboken för tekniska informations- och cybersäkerhetsövningar är skriven med utgångspunkt i Myndigheten för samhällsskydd och beredskaps (MSB:s) existerande övningshandbok Öva krishantering – Handbok i att planera, genomföra och återkoppla övningar och bygger erfarenheter från tidigare tekniska informations- och cybersäkerhetsövningar.
Bland handbokens rekommendationer återfinns följande praktiska råd och tips:

- Utgå från övningsuppdragets direktiv och sätt genomförbara och mätbara mål med övningen. Ha inte för många mål. Använd direktivdialogen för att se om givna resurser täcker syftet med övningen. Om inte behöver ambitionen eller övningen möjligen begränsas för att hållas inom givna ramar, alternativt ytterligare resurser tillskjutas.
- Ha med rättsliga aspekter med avseende på informationshantering och övningsdokumentation, såsom säkerhet och sekretess, under hela projektlednings- och övningsprocessen (från planering, via genomförande och utvärdering samt uppföljning/återkoppling). Beakta tid för upprättande av avtal och överenskommelser mellan övningens parter i planeringen för övningen.
- Använd gärna och uppdatera kontinuerligt en risk- och konsekvensanalys. Denna kan användas för att åskådliggöra förutsedda och oförutsedda risker med övningen. Tekniska informations- och cybersäkerhetsövningar är ofta komplexa till sin struktur vilket kräver relativt stora resurser i tid, personer och kapital (inköp av hårdvara och mjukvara m.m.).
- Tänk på att inkludera såväl den tekniska ledningen för stöd och samband (ansvarig för infrastrukturen i informations- och cybersäkerhetsövningen) som utvärderingsledningen i övningsplaneringen *och* definitionen av syfte och mål.
- Med god planering – projektledning som bemannar, upprättar och kan följa upp beslutad ansvars- och rollfördelning, planerings- och genomförandeorganisation samt utvärderingsorganisation – kan denna lägga grunden för ett väl strukturerat genomförande.
- Tänk på att även ha koordinatorer för övningsprojektets informationshantering, samt en medie- och kommunikationsansvarig för besökare.
- Beakta spårbarhet med avseende på informations- och kommunikationshantering samt övningsdokumentation.
- Tekniska övningar kräver möjlighet till uppdaterade lägesbilder samt omfattande testning av övningsmiljön och dess system före övningen startar.
- Sist men inte minst, tänk på att tekniska informations- och cybersäkerhetsövningar samtidigt handlar om människor. Om möjligt, se gärna till att hålla kontinuerliga planeringsmöten och konferenser med inblandade deltagare så att dessa får möjlighet att träffas såväl under planeringen som under genomförandet och uppföljningen av övningen.

Referenser och litteraturförslag

Baltic Cyber Shield Cyber Defence Exercise 2010, After Action Report. For Public Use. Tillgänglig via: https://www.fhs.se/sv/forskning/centrumbildningar-och-forskningsprogram/cats/nyheter-och-artiklar/2010/ (publicerad 2010-10-06).

Europeiska kommissionen (2009) Meddelande från Kommissionen till Europaparlamentet, Rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén om skydd av kritisk informationsinfrastruktur, 'Skydd mot storskaliga IT-attacker och avbrott: förbättrad beredskap, säkerhet och motståndskraft i Europa'". EG-kommissionen, KOM(2009) 149 slutlig. Bryssel den 30 mars 2009.

Karlsson, J. (2010) "Rapport efter CCD COE – Swedish CDX 2010", Mj J. Karlsson, intern rapport till MSB, Försvarshögskolan, Centrum för asymmetriska hot- och terrorismstudier, maj 2010.

Lag (1990:409) om skydd för företagshemligheter.

Lag (2006:544) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap (LEH).

Lag. Offentlighets- och sekretesslagen (2009:400).

MSB (2011) Ett fungerande samhället i en föränderlig värld, Nationell strategi för skydd av samhällsviktig verksamhet. DanagårdLiTHO, MSB266, Maj 2011.

MSB (2011) Nationell hanterandeplan för allvarliga IT-incidenter, Svar på regeringens uppdrag till Myndigheten för samhällsskydd och beredskap, (Fö2010/701/SSK, Regeringsbeslut 12,2010-04-14). Datum 2011-03-01, diarienr 2010-4545.

MSB (2010) Strategi för samhällets informationssäkerhet, 2010-2015. MSB, Karlstad.

MSB (2010) *Utvärdering av övningar*, Myndigheten för samhällsskydd och beredskap. Danagårds Grafiska AB, 2010. (Tillgänglig via: http://www.msb.se/RibData/Filer/pdf/25490.pdf, 2011-05-09.)

MSB (2009) *Öva Krishantering – Handbok i att planera, genomföra och återkoppla övningar",* Myndigheten för samhällsskydd och beredskap. (Tillgänglig via: http://www.msb.se/RibData/Filer/pdf/25608.pdf, 2010-10)

SIS, *Terminologi för informationssäkerhet*, SIS HB 550, utgåva 3. SIS Förlag AB, Elanders: 2007.

Merriam Webster, tillgänglig via: http://www.merriam-webster.com/

Nationalencyklopedin, tillgänglig via: http://www.ne.se/

OTRS, tillgänglig via: http://www.otrs.org

Wikipedia, tillgänglig via: http://sv.wikipedia.org/wiki/

Myndigheten för samhällsskydd och beredskap
651 81 Karlstad Tel 0771-240 240 www.msb.se
Publ.nr MSB 433 ISBN 978-91-7383-255-7