Facilitators guide til cyberdilemmaøvelse

Øvelsen er udarbejdet af Beredskabsstyrelsens Center for Uddannelse i samarbejde med Center for Cybersikkerhed

Dette dokument bør læses forud for gennemførelsen af dilemmaøvelse cybersikkerhed.

Guide til dilemmaøvelse 'Cybersikkerhed'

Velkommen til Beredskabsstyrelsens 'klar til brug' øvelse, der handler om cybersikkerhed. Denne guide indeholder al den nødvendige information du skal bruge, når du skal i gang med planlægningen af dilemmaøvelsen om cybersikkerhed. Guiden indeholder en beskrivelse af rollen som facilitator under gennemførelsen af øvelsen og gode tips til, hvordan du kan gribe evalueringen og opfølgningen på øvelsen an. Guiden følger planlægning-, gennemførelse- og evaluering af øvelsen som struktur.

Denne øvelse er designet som en forberedende øvelse i forbindelse med den nationale krisestyringsøvelse KRISØV 2013. Scenariet for KRISØV 2013 vil handle om en række cyberhændelser og derfor vil fokus for denne dilemmaøvelse også være cyberrelaterede hændelser. Øvelsen kan også anvendes som en almindelig dilemmaøvelse med et scenarie der handler om cybersikkerhed.

Formålet med at udvikle 'Klar-til-brug' dilemmaøvelser er, at muliggøre afholdelse af dilemmaøvelser, der har fokus på at klarlægge roller, ansvar og håndtering af ekstraordinære hændelser uden at anvende mange timer på planlægning af øvelsen. Målet med denne dilemmaøvelse er, at forberede myndigheder på deltagelse i KRISØV 2013, hvis hovedscenarie handler om et større koordineret cyberangreb på Danmark. Hændelserne i denne øvelse er holdt på et overordnet niveau således at øvelsen kan anvendes af en bred kreds af både private og offentlige beredskabsaktører.

Øvelsen er designet af Beredskabsstyrelsen i samarbejde med Center for Cybersikkerhed (CfCS) under Forsvarets Efterretningstjeneste.

Efter gennemførelsen af øvelsen vil øvelsestagerne have haft mulighed for:

- At klarlægge roller og ansvar i organisationen i forbindelse med håndtering af cyberhændelser.
- At bedømme paratheden i organisationens evne til at håndtere cyberhændelser
- At have opnået en bedre forståelse for hvilken indvirkning cyberhændelser kan have for organisationens drift og opgavevaretagelse.
- At afprøve beredskabsplaners anvendelighed i forbindelse med cyberhændelser.

Øvelsens indhold
Øvelsen består af 5 moduler (0-4), som hver især sætter fokus på en bestemt cyberhændelse. I hvert modul lægges endvidere særlig vægt på håndtering af en eller flere af kerneopgaverne:

- 1. Aktivering af drift af stab
- 2. Håndtering af informationer om krisen
- 3. Koordinering af handlinger og ressourcer
- 4. Krisekommunikation
- 5. Operativ indsats (Ikke medtaget i dilemmaøvelsen)

Kerneopgaverne er nærmere beskrevet i Beredskabsstyrelsens publikation Helhedsorienteret Beredskabsplanlægning (HOB).

Øvelsens varighed kan variere alt efter deltagerantal, om I vælger at bruge alle moduler og hvor meget tid I har til rådighed til gennemførelse af øvelsen. Øvelsen designet til at vare ca. 2-4 timer, men det er op til øvelseslederen at fastlægge det forventede tidsforbrug.

Dette dokument bør læses forud for gennemførelsen af dilemmaøvelse cybersikkerhed.

Overblik over øvelsens moduler, kerneopgaver og tidsforbrug

Modul	Kerne opgave	Tid	Slides	Indhold
Velkomst		20 min.	1-5	• Velkomst • Dagens agenda • Hvorfor øve cyberhændelser • Øvelsens formål og mål • Spilleregler under øvelsen
Modul 0 Krisestyring ved cyberhændelser	Planlægningsgrundlag (Helhedsorienteret beredskabs-planlægning)	10 min.	6	• Planlægningsgrundlag
Modul 1 DDoS-angreb	1. Aktivering og drift af krisestab	30 min.	7-8	• Præsentation af hændelsen: DDoS-angreb • Diskussion
Pause		10-15 min.	9	
Modul 2 Kompromittering af data	2. Håndtering af informationer om krisen. 3. Koordinering af handlinger og ressourcer	30 min.	10-11	• Præsentation af hændelsen: Kompromittering af data • Diskussion
Modul 3 Servernedbrud	4. Krisekommunikation	30 min.	12-13	• Præsentation af hændelsen: Servernedbrud • Diskussion
Pause		10-15 min.	14	
Modul 4 Sikkerhedsprocedurer	Forebyggelse, uddannelse og øvelser (Helhedsorienteret beredskabs-planlægning)	20 min.	15-16	• Præsentation af hændelsen: Sikkerhedsprocedurer • Diskussion
Debriefing	Evalueringer (Helhedsorienteret beredskabs-planlægning)	30-35 min.	17-18	• Debriefing af øvelsen • Identifikation af læringspunkter
Afslutning		5 min.	19	• Videre arbejde med evaluering og implementering af læringspunkter

Planlægning af øvelsen

Forud for øvelsens afholdelse bør ledelsen i organisationen orienteres og godkende øvelsens samlede anvendelse af ressourcer, formål og mål samt placere ansvaret for, hvem der skal

implementere de læringspunkter øvelsen afstedkommer. Herefter anbefales det at udpege en ansvarlig for øvelsen (øvelsesleder), som har ansvaret for at planlægge og gennemføre øvelsen, hvilket betyder, at øvelseslederen også skal fungere som facilitator under øvelsen. Evt. kan der udpeges en ansvarlig for debriefing og evaluering af øvelsen, men rollen kan også varetages af øvelseslederen. Det anbefales dog, at der som minimum er udpeget en person, der kan tage noter/føre log undervejs, da facilitator ikke både kan styre øvelsen og notere læringspunkter mv.

Deltagerne

Dilemmaøvelsen er designet til at deltagerne i øvelsen udgøres af organisationens krisestab. Øvelsen er ikke en teknisk øvelse, men en øvelse, der fokuserer på organisationens generelle kapacitet til at håndtere cyberhændelser. Deltagerkredsen behøver derfor ikke at have særlig kendskab på IT-området. Det anbefales dog at organisationens IT-ansvarlige og ansvarlige for sikkerhed og beredskab deltager.

Beredskabsstyrelsen anbefaler at øvelsen gennemføres som en varslet øvelse, hvor deltagerne på forhånd kender formål og mål med øvelsen og at scenariet omhandler cyberhændelser, men ikke kender detaljerne i scenariet. Ved at øvelsen er varslet sikrer øvelseslederen at alle kan deltage og har sat tid af til øvelsen i deres kalender.

Logistik

Dilemmaøvelsens gennemførelse kræver ikke meget logistik. For at gennemføre øvelsen er der brug for:

- Et lokale (gerne organisationens krisestyringsfaciliteter, ellers kan et almindeligt mødelokale anvendes) med overhead projekter og lærred til brug for visning af power point.
- Computer med power point showet på.
- Kuglepenne, blokke, tavler, flip over med tusser, navneskilte til bordet.
- Kopier af slides vedr. præsentationer af hændelserne (Slides nr. 6, 7, 8, 10-13, 15-18) Bemærk at slides bør ikke uddeles på forhånd, men undervejs i øvelsen, når de relevante slides er blevet præsenteret.
- Forplejning (Kaffe, the, vand, frugt mv.)

Opgaveliste

Fase	Opgave	Ansvar
Planlægning	• Få ledelsens accept for at afholde øvelsen.	Ledelse/Øvelsesleder
	• Fastlæg dato.	Øvelsesleder
	• Book mødelokale	Øvelsesleder
	• Identificer og inviter deltagere.	Øvelsesleder
	• Vær fortrolig med denne guide og de publikationer der er listet op under litteraturlisten.	Øvelsesleder
	• Udpeg evt. en evaluator	Øvelsesleder
	• Gennemgå power point show og tilret til de lokale forhold.	Øvelsesleder
	• Tilrettelæg	Evaluator

	evalueringsfasen af øvelsen.	

Gennemførelse og debriefing af øvelsen

Sørg for at afprøve teknikken inden øvelsen starter. Når alle deltagere er ankommet starter øvelsen med at du som øvelsens facilitator introducerer dig selv og din rolle under øvelsen. Introducer de øvrige funktioner (log-fører, evaluator mv.)
Som facilitator er det dit ansvar at øvelsen forløber som planlagt. Derfor er det vigtigt at du styrer øvelsen efter en tidsplan, så du sikrer at deltagerne når alle øvelsens elementer. Hvis tidsplanen skrider, er det oftest debriefingen, som ikke gennemføres helt eller fuldstændig udelades, hvilket ikke er formålstjenligt. Nedenfor er listet et par gode råd til at sikre at tidsplanen overholdes:

- Forbered gennemførelsen af øvelsen grundigt og sæt dig ind i de publikationer der er foreslået i litteraturlisten.
- Øv timingen af slides og sørg for at du ikke bruger længere tid end planlagt på fx at introducere hændelserne.
- Styr talerækken under øvelsen.
- Bed deltagerne om at 'parkere' længerevarende diskussioner eller emner, der ligger uden for øvelsens formål og mål. De kan tages op til slut i øvelsen, hvis der er tid eller evt. tages op på et særskilt møde efter øvelsen.
- Spørgsmål og blindgyder (situationer, hvor deltagerne ikke kan komme videre i diskussionen grundet forhold der skal undersøges nærmere) skal noteres ned og tages op i debriefingen eller evalueringen af øvelsen.

Øvelsen indeholder ikke et komplet evalueringskoncept, men indeholder kun den debriefing (også kaldet Hot Wash), der afholdes umiddelbart efter øvelsen. Øvelseslederen bør i samarbejde med den evalueringsansvarlige beslutte, hvordan den efterfølgende evaluering skal gribes an. Du kan læse mere om evaluering af øvelser i National øvelsesvejledning på øvelsesforum.dk, hvor der også er forslag til, hvordan en debriefing af en øvelse kan gribes an.

Opgaveliste

Fase	Opgave	Ansvar
Gennemførelse	• Afprøv teknik	Facilitator
	• Byd velkommen og introducer til øvelsens formål og mål.	Facilitator
	• Præsentationsrunde af facilitator, evalueringsansvarlig og øvrige deltagere i øvelsen.	Facilitator
	• Gennemfør modulerne i øvelsen jf. power point show.	Facilitator
Debriefing	• Begynd med at introducere debriefing-fasen jf. power point show.	Evaluator
	• Del øvelsesdeltagerne op i mindre grupper eller i par.	Evaluator
	• Gennemgå de enkelte	Evaluator

	elementer i kerne-opgaverne, som I har valgt at ligge fokus på, og bed deltagerne om at forholde sig til dem i deres diskussioner.	
	• Gennemgå deltagernes tilbagemeldinger og fasthold læringspunkter på tavle eller flip over.	Evaluator
	• Informer deltagerne om den videre proces i evalueringen og implementering af læringspunkter i organisationen	Evaluator

Evaluering og opfølgning på øvelsen

Øvelsen evalueres jævnfør de fastsatte mål, men vær ikke bleg for at inddrage relevante pointer, der opstår undervejs i øvelsen. Evalueringen gennemføres med udgangspunkt i debriefingen og de observationer evaluator har gjort under øvelsen. Man kan også anvende spørgeskemaer eller interviewe deltagerne efterfølgende eller samle nøglepersonel til et evalueringsseminar. Herefter dokumenteres evalueringen i en evalueringsrapport (Se skabelon for opstilling af evalueringsrapport i National øvelsesvejledning).

Opgaveliste

Fase	Opgave	Ansvar
Evaluering og implementering af læring	• Fastlæg rammerne for evalueringen af øvelsen med den øvrige øvelsesledelse	Evaluator/Øvelsesleder
	• Fastlæg evaluerings-seminar ca. en uge eller to efter øvelsen.	Evaluator
	• Inviter nøglepersonel til evalueringsseminaret.	Evaluator
	• Gennemfør evt. evalueringsseminar og fastlæg læringspunkter og opstil forslag til implementering af læringspunkter jf. Aktionsskema (Se aktions-skema i litteraturlisten).	Evaluator
	• Skriv evalueringsrapport og del med deltagerne og organisationen	Evaluator
	• Iværksæt implementering	Ansvarlig for implementering

	af læringspunkter og følg op med passende interval	af læringspunkter

Litteraturliste

Aktionsskema:

Lærings-punkt	Anbefaling (hvad)	Deltagere (hvem)	Aktivitet (hvordan)	Ansvar	Opmærksom-hedspunkt	Tid
Ekstern Krisekom-munikation ikke koordine-ret	Skærpet fokus på ansvar for koordinering af ekstern krisekom-munikation	De lokale beredskabsstabe	Seminar om krisekommunika tion	Leder af den lokale beredskab sstab	Inddragelse af hele ledelses-niveauet	18. jan. 2013
	Afholdelse af dilemma-øvelse om krisekom-munikation	Repræsentanter fra eksterne organisationers kommunikations afdelinger	Dilemmaøvelse afholdes med fokus på koordinering af kommunikations faglige udfordringer og dilemmaer	Kommuni-kations-ansvarlig for fx politikreds	Kræver ekstern bistand	3. mar. 2013

Dette dokument bør læses forud for gennemførelsen af dilemmaøvelse cybersikkerhed.

Center for Cybersikkerhed (CfCS):

- Risikovurdering 2012: http://fe-ddis.dk/cfcs/CFCSDocuments/Risikovurdering2012.pdf
- Seneste trusselsvurdering: http://fe-ddis.dk/cfcs/Situationsbilleder/Pages/Situationsbilleder.aspx
- Situationsbillede af sikkerhedstilstanden på internettet april 2013: http://fe-ddis.dk/cfcs/CFCSDocuments/Situationsbillede%20-%20April%202013.pdf

Beredskabsstyrelsen (BRS):

- Helhedsorienteret beredskabsplanlægning (HOB): http://brs.dk/viden/publikationer/Documents/HOB-vejledning.pdf
- Nationalt Risikobillede (NRB): http://brs.dk/viden/publikationer/Documents/Nationalt_Risikobillede.pdf
- National øvelsesvejledning (NØV): http://øvelsesforum.dk/Dokumenter/Øvelsesvejledning/National%20øvelsesvejledning.pdf

Politiets Efterretningstjeneste (PET):

- Politiets efterretningstjeneste (PET) publikation vedr. Informationssikkerhed https://www.pet.dk/Forebyggende%20sikkerhed/~/media/Forebyggende%20sikkerhed/AFS_publikationer/informationssikkerhedpdf.ashx