Gjennomførings-direktiv

 Øvelse XX kommune xx.xx.xxxx

 Utarbeidet av øvingsledelsen

Innholdsfortegnelse

[1 Bakgrunn 3](#_Toc168053859)

[2 Føringer 3](#_Toc168053860)

[3 Hensikt 4](#_Toc168053861)

[4 Suksesskriterier for krisehåndtering 4](#_Toc168053862)

[5 Målsetting 4](#_Toc168053863)

[6 Øvingsmomenter 5](#_Toc168053864)

[6.1 Tydelighet i roller og ansvar 5](#_Toc168053865)

[6.2 Stabsarbeid 5](#_Toc168053866)

[6.3 Informasjonshåndtering 5](#_Toc168053867)

[6.4 Planverk og faglighet 6](#_Toc168053868)

[6.5 Hendelseshåndtering systemene 6](#_Toc168053869)

[6.6 Ønsker fra xx kommune: 6](#_Toc168053870)

[7 Scenario for øvelsen 6](#_Toc168053871)

[8 Gjennomføring 7](#_Toc168053872)

[8.1 Program 7](#_Toc168053873)

[8.2 Deltakelse fra organisasjonen 8](#_Toc168053874)

[8.3 Øvingsledelse, spillstab og teknisk support 8](#_Toc168053875)

[8.3.1 Rom og utstyr opplæring og øvelse 9](#_Toc168053876)

[8.3.2 Spillmeldinger øvelse 9](#_Toc168053877)

[8.3.3 Nettaviser og sosiale medier 10](#_Toc168053878)

[8.4 Bevertning 10](#_Toc168053879)

[9 Oppsummering og vurdering 10](#_Toc168053880)

[Referanser 11](#_Toc168053881)

# Bakgrunn

I Grethe Østby sitt doktorgradsarbeid (Østby, 2023) ble det utarbeidet et **konsept** for gjennomføring av kombinert kriseledelse, og en teknisk hendelseshåndteringsøvelse (i et IKT-miljø). En kriseledelsesøvelse er eksempelvis som gjennomført i henhold til Lov om kommunal beredskapsplikt, sivile beskyttelsestiltak og Sivilforsvaret. En teknisk hendelseshåndteringsøvelse kalles på ‘fagspråket’ gjerne en ‘incident response’ øvelse dersom systemene er angrepet, eller en ‘disaster recovery’ øvelse dersom systemene er ødelagt. Sistnevnte kan være dersom et datasenter har vært utsatt for jordskjelv og alle data lagret ved datasenteret er borte for alltid.

Konseptet utarbeidet av Østby baserer seg i stor grad på et cyber-angrep hvor man kombinerer kriseledelse i en organisasjon sammen med operativ teknisk hendelseshåndtering i datasystemer. Det vil si at man øver seg på en tilsvarende hendelse slik som Østre Toten ble utsatt for. Dette konseptet krever et scenario som er både teknisk og organisasjonsmessig tilpasset den enkelte organisasjon og det nivået av modenhet den enkelte organisasjon befinner seg på. Dette betyr å innhente opplysninger fra kommunene for å utarbeide leksjoner, øvelser og deri scenarioer tilpasset modenheten i organisasjonen. I tillegg betyr det et samarbeid med en cyber-range for å etablere en teknisk øvingsplattform hvor IKT-sikkerhetspersonellet i organisasjonen blir ‘utsatt’ for hendelsen så realistisk som mulig.

En cyber-range er en arena der testing, opplæring og trening er verktøy for å eksponere personer, bedrifter og virksomheter for tilnærmet realistiske hendelser og situasjoner i et trygt miljø. En slik arena bør sikre effektiv kompetansebygning basert på erfaring og observasjon fra virkeligheten.

Det er fullskalaøvelse med opplæring for xx kommune xx.xx.xxxx.

xx har ansvaret for planleggingen og gjennomføringen av øvelsen. Det vil si opplæring, lage dreieboka og sørge for spill og mediestab.

# Føringer

Det er ikke gitt noen spesielle føringer fra sentrale myndigheter for disse øvelsene. Det er allikevel et par viktige forhold som skal bringes inn i øvelsen:

* Rollene som skal øves er kriseledelse, informasjonsavdeling, førstelinje (servicetorg), taktisk og de man normalt sett ville hatt med i en krisehåndteringsøvelse av denne sorten fra xx kommune, samt operativt IKT-personell som normalt vil håndtere sikkerhetshendelser, slik at spillstab dermed kan spille de rollene de normalt ville gjort under en fullskalaøvelse
* bruk av RAVYN som stabsstøtteverktøy (loggføring, oppgavefordeling, meldinger og rapportering).
* bruk av xx som SIEM-verktøy
* bruk av xx som media-verktøy
* bruk av en cyber-range/kommunetilpasset for drift av system som blir angrepet
* bruk av en cyber-range/kommunetilpasset for å sikkert gjøre injeksjoner/eksfiltrasjon på en sikker måte

# Hensikt

Øvelsen skal legges opp til at deltakere skal ha en mestringsfølelse i etterkant slik at man ved en hendelse kan si «dette har vi øvd på slik at dette fikser vi».

Øvelsen også gi spillstaben erfaring i å gjennomføre denne type øvelser, samt sjekke ut tekniske løsninger – ikke minst for sikkerhet. Gjennom egne øvelseserfaringer og evalueringer, skal spillstab og teknisk personell bli bevisst eventuelle potensialer for videre utvikling, både i forhold til tilnærming til eksterne organisasjoners planverk, kompetanse og utøvelse (selv om kompetanse og utøvelse i denne sammenheng vil komme i annen rekke).

# Suksesskriterier for krisehåndtering

Direktoratet for samfunnssikkerhet og beredskap har samlet og evaluert erfaringer fra krisehåndteringssituasjoner nasjonalt og internasjonalt. Resultatet av dette arbeidet har bl.a. resultert i et ‘sett’ suksesskriterier som ofte vil være grunnleggende forutsetninger for å kunne håndtere kriser. Det forutsettes at spillstab gjør seg kjent med disse, og nytter disse under øvelsen.

* Lederrollen
* Ansvar og roller
* Etablert planverk inklusive informasjonsstrategi
* Varslingsrutiner
* Omsorg for rammede og berørte
* Samordning og koordinering
* Evne til improvisasjon og handling under press

Det forutsettes at spillstab gjør seg kjent med disse, og observerer og gir sine innspill ift. disse under øvelsen. Se punkt 6 øvingsmomenter for nærmere detaljer. For denne type øvelser spesielt er det laget en egen presentasjon med suksesskriterier. Se vedlegg 1, Sjekkliste infosec ledelses øvelser.

# Målsetting

Øvelsen skal i utgangspunktet gi organisasjonen som øves nødvendig grunnlag for å i ettertid kunne vurdere kvaliteten av overordnet beredskapsplan, men også gjøre seg kjent med informasjonssikkerhetsstrategi, policyer, instrukser og rutiner, GDPR/personvern, risikostyring av informasjonssikkerhet, vedlikeholdsarbeid for informasjonssikkerhet, samt evne til å håndtere krisen på teknisk nivå (gjenopprettelse). Det legges spesiell vekt på:

* rolleforståelse og ansvarsavklaring mellom avdelingene og eksterne som Statsforvalter, politi, Datatilsynet, kommuneCERT, NSM og PST, samt innad i kriseledelsen
* organisering, vurderings- og beslutningsevne, rutiner, tilrettelegging og bruk av sentrale hjelpemidler og verktøy (eksisterende)
* bruk av relevant planverk, samt fagligheten i krisehåndteringen
* strategier og rutiner knyttet til informasjons- og kommunikasjonshåndtering
* eskalering av informasjon i krisehåndtering – deri tilbakemeldinger på beslutninger
* mediehåndtering

# Øvingsmomenter

Som nevnt under punkt 5 vil det under øvelsen settes søkelys på områder som roller og ansvar, stabsarbeid, faglighet og informasjon. Øvingsmomenter er en konkretisering av hensikt og målsetting, og vil danne grunnlag for alle innspill under øvelsen. **Spillstabens roller er i dette kapittelet beskrevet som de rollene de faktisk skal spille.**

## Tydelighet i roller og ansvar

* Er det en klar og tydelig avklaring av roller og ansvar mellom **kriseledelse, taktisk ledelse og operativ ledelse**?
* Er **kriseleder** i xx kommune tydelig i rollen som ”**stabssjef**”?
* Er de **øvrige medlemmene i kriseledelsen** bevisst på sine roller og oppgaver?
* Er det en god og tydelig rolle- og ansvarsforståelse mellom **kriseledelsen vs.** **eksterne,** slik som **Statsforvalter, politi, Datatilsynet, kommuneCERT, NSM, PST**?
* Er det en god og tydelig rolle- og ansvarsforståelse mellom **kriseledelsen i xx kommune vs. kommunens øvrige virksomhetsområder og/eller andre ytre aktører (eksempelvis systemleverandører)?**

## Stabsarbeid

* Klarer organisasjonen å **etablere og organisere kriseledelse** på en rask og god måte?
* Er det **tilstrekkelig** **bemanning**? (spesielt på taktisk og operativ ledelse for IKT-sikkerhet/gjenoppretting)
* Hvordan gjennomfører staben **informasjonsinnhenting** og **situasjonsanalyse**?
* Klarer beredskapsledelsen å **holde fokus**? (skille mellom det vesentlige og det mindre vesentlige innspill fra spillstaben)
* Klarer strategisk ledelse å **fatte beslutninger** **og få dem iverksatt**?
* Hvordan er kriseledelsens **oversikt** og **samordning** av tilgjengelige ressurser i og utenfor xx kommune (lister over evakueringssteder, andre helseinstitusjoner, men også redundans på systemer/bruk av systemer fra andre steder etc.)?
* Hvordan er de **generelle rutinene** og bruk av hjelpemidler, herunder bruk av Raven? (loggføring, tavler, kart, stabsmøter, meldingsfordeling, telefonbruk mv.)
* Hvordan er de **generelle rutinene** ift. eskalering av hendelser (SIEMS og møtepunkter) og tilbakemelding av beslutninger?

## Informasjonshåndtering

* Har organisasjonen en tydelig **mediestrategi** som gjennomsyrer alt informasjons- og kommunikasjonsarbeid i en beredskapssituasjon?
* Håndterer organisasjonen **henvendelser** fra pårørende, presse og publikum (telefon og/eller direkte oppmøte), på en god måte?
* Har organisasjonen etablert gode rutiner for å **overvåke medieomtale**? (overvåke, håndtere og bruke strømmen av informasjon fra nettaviser, radio, TV og sosiale medier)
* Er det en tydelig og klar **ansvarsdeling** i strategisk ledelse når det gjelder hvem som informerer om hva, når og i hvilke kanaler? (ordfører, kommunikasjonsansvarlig, fagansvarlige IKT, politi, andre)
* Er det god **informasjonsflyt** mellom kriseledelse og sentralbord? (bla. siling/ikke siling, og førstelinjen som informasjonsledd)
* Brukes **pressekonferanser/pressemøter** i samsvar med organisasjonens mediestrategi? (hyppighet, tilrettelegging, deltakelse, tidsbruk mm.)
* Brukes foretakets **nettside**, **pressemeldinger**, **e-post**, **SMS** el. i samsvar med organisasjonens mediestrategi? (hyppighet, budskap, relasjoner til andre)
* Benyttes **sosiale medier** i samsvar med organisasjonens mediestrategi? (informasjon inn eller ut, form, innhold og målgruppe)

## Planverk og faglighet

* Har organisasjonen **relevante planverk** tilgjengelig, og blir dette benyttet på en hensiktsmessig måte?
* Vurderes de benyttede planverk som et hensiktsmessig verktøy, og er planen(e) **tilstrekkelig oppdatert**?
* Ivaretas **fagligheten** i vurderinger og beslutninger?
* Hvilke systemer vil være tilgjengelige ved et angrep?
* Hvilke systemer må man ‘andre steder’ (det vil si annet fysisk oppmøte) for å hente opplysninger fra?
* Hvordan gjennomføres plan for gjenoppretting (hva er maksimal nedetid)?

## Hendelseshåndtering systemene

* Sporing/søk i logger basert på varsler i SIEM-verktøyet
* Ivaretakelse av logger og loggføring
* Back-up -> flytte data (øve på dette)
* Benytte brannmur-informasjon (varsler)/brannmuradministrasjon
* Isolering av systemer (kan også være at man blir isolert fra samarbeidspartnere)
* Gjenoppretting
* Registrering/loggføring av markører/infiltrering/avvik – hvor og hvordan, og eskalering/distribusjon av denne type informasjon
* Situasjonsbrief for kriseledelse
* Iverksettelse av tiltak besluttet i kriseledelse - fremdriftsplaner
* Samspill mellom operativ og/eller teknisk ledelse opp mot etterforskere, kommuneCERT og evt. NSM (og øvrige ved Nasjonalt cybersikkerhetssenter) – hva skal hhv. operativ ledelse, taktisk ledelse og kriseledelse kommunisere/hvem har ansvar for hva?

## Ønsker fra xx kommune:

* …

# Scenario for øvelsen

Scenario vil være bestemmende for hvilke deler av organisasjonens virksomhetsområder som berøres, og er valgt ut fra en virksomhetsanalyse, samt andre innspill fra xx kommune som beskrevet i (Østby, Berg, et al., 2019; Østby & Kowalski, 2020). Øvelses-scenarioet vil ikke bli gjort kjent for organisasjonen før øvelsesstart.

Scenario vil så langt som råd er, ta utgangspunkt i reel tid, og den faktiske politiske og de system-sikkerhets-utfordringer som eksisterer på øvelsesdagen.

# Gjennomføring

**Øvelsen gjennomføres som en fullskala-øvelse, og er rettet mot organisasjonens håndteringsevne ved en informasjonssikkerhetshendelse. Øvelsen er en full-skala øvelse, dvs. for både strategisk ledelse, operativ ledelse og utvalgte roller fra taktisk ledelse, tilsvarende som beskrevet i** (Østby & Katt, 2019)**.**

Samarbeidspartnere som kan inviteres inn på øvelser er slike som Statsforvalter, politiet, kommuneCERT, NSM og NC3. Disse kan også spilles av kompetente personer i spillstab. Roller i situasjonen, mediestab og red-team spilles av på forhånd utpekte personer.

Organisasjonens rutiner for innkalling ved oppstått hendelse brukes. Det forutsettes at strategisk ledelse på forhånd er varslet slik at de er på plass og at det ikke brukes tid på at disse skal komme seg til lokalene ved valgte cyber-range.

**Under selve øvelsen forutsettes det at organisasjonene tar reel kontakt med øvrig deler av organisasjonene som deltar på øvelsen eller spillstab (som spiller resten av verden) for å innhente nødvendig informasjon til kriseledelsen som kan være nødvendig beslutningsgrunnlag**. **Husk å starte alle forespørsler med øvelse, øvelse, øvelse!** Vurdering og iverksettelse av tiltak skal altså basere seg på reelt innhentet informasjon øvelsesdagen– ikke på egne premisser.

Organisasjonen må fysisk legge ut relevant informasjon som for eksempel nettsaker på plattformer tilrettelagt for dette.

## Program

Tidspunktene i programmet vil ut fra øvelsens gang kunne variere noe, men aktivitetene vil ikke gå ut over den ytre tidsrammen.

 **xx.xx.xxxx**

|  |  |
| --- | --- |
| 09:45 – 10:00 | Oppmøte og registrering Sted (kaffe og wienerbrød) |
| 10.00 - 11.00 | Krav til samfunnssikkerhet og beredskap ved informasjonssikkerhets-hendelser (lover, forskrifter, veiledere og oppdragsbrev), og andre informasjonssikkerhets-oppgaver organisasjonen kan være forberedt på. |
| 11:00 - 11:10 | Hente-kaffe-pause |
| 11:10 – 12:00  | Kriseledelse og stabsarbeid: Situasjonsanalyse, ressursbehov (personell og materiell), rollefordeling og operativ oppfølging ved informasjonssikkerhetshendelser | Operativt team starter øvelse. Arbeid med utarbeidelse av situasjonsbrief i cyber-range (Sted). |
| 12:00 – 12:45 | Lunsj kantina |
| 12:45 – 13:30 | Informasjonsberedskap, leder-brief, krisekommunikasjon, RAVYN og SIEMS |
| 13:30 – 15:00 | Status i dag, ROS-analyser, beredskapsplaner, tiltakskort roller |
| 15:00 – 15:15 | Brief fra operativt team til ledelse (innledning til felles-øvelse – Sted) |
| 15:15 – 16:00 | Middag (kantina) |
| 16:00 – 18:45 | Felles øvelse starter (cyber-range) |
| 18:45 – 19:00 | Situasjonsanalyse fra instruktør (cyber-range) |

 **xx.xx.xxxx**

|  |  |
| --- | --- |
| 08:30 | Registrering |
| 08:30 – 11:00 | Øvelse fortsetter ved NCR |
| 11:00 – 11:45 | Evaluering |
| 11:45 – 12:30 | Lunsj (kantina)  |
| 12:30 – 13:00 | Hotwash sesjon (med en liten filmsnutt) og gjennomgang av evaluering |
| 13:00 | Takk for nå, og vel hjem! |

## Deltakelse fra organisasjonen

xx kommune:

…

## Øvingsledelse, spillstab og teknisk support

Øvelsen ledes av instruktører, spillstab og teknisk support.

Instruktører vil være:

Strategisk og taktiske team: xx

Operative team: xx

Følgende roller vil dekkes av spillstab:



**Figur 1.** Spillstab fullskalaøvelser ved informasjonssikkerhetshendelser (Østby, Lovell, et al., 2019)

Spillstab vil være (avhengig av hvem som kan delta):

Leder: xx

Samarbeidspartnere spilles av: xx

Roller i situasjonen spilles av: xx

Red-team kan spilles av: xx

Medie-staben kan spilles av: xx

Teknisk support-team på denne øvelsen vil være: xx

Praktisk gjennomføring: …

Spillstabmedlemmer som ikke kan delta på disse øvelsene som en del av sin «normale» lønn og sitt «normale» samfunnsoppdrag vil inngå egne avtaler med cyber-range om dette.

### Rom og utstyr opplæring og øvelse

Det er behov for rom til å gjennomføre opplæring (tirsdag), og det er behov for å benytte cyber range for øvelse (tirsdag og onsdag).

### Spillmeldinger øvelse

Spillmeldinger og henvendelser under øvelsen kan formidles skriftlig via e-post, telefon (som deles ut under øvelsen), RAVYN, eller på annen direkte måte. For å unngå eventuelle misforståelser er det viktig å være tydelig på at det dreier seg om en øvelse.

* ALLE meldinger skal tydelig merkes ØVELSE – ØVELSE – ØVELSE.

### Nettaviser og sosiale medier

Det er kun lokale systemer ved cyber-range som skal benyttes i sammenheng med øvelsen. … Følgende verktøy benyttes som nettaviser og sosiale medier:

## Bevertning

Øvingsledelse serverer kaffe/te/mineralvann samt litt å bite i ved frammøte, og for øvrig måltider i henhold til program.

# Oppsummering og vurdering

(Onsdag) etter lunsj gjennomføres det en stedlig todelt oppsummering og gjennomgang av førsteinntrykk (Hotwash) etter øvelsen (Ebrahimian et al., 2021; Vykopal et al., 2018), men først en evaluering direkte knyttet til målsettingene og øvingsmomentene i gjennomføringsdirektivet:

* del én – 1) Kriseledelse (xx ansvarlig), 2) Operativt IKT-team/IRT (xx ansvarlig) og 3) spillstab og øvingsledelse og teknisk team (xx ansvarlig) deles i tre grupper og gjennomfører evaluering basert på øvingsmomenter.
* delt to – Hotwash (felles).

Det er viktig at samtlige som på en eller annen måte har bidratt under øvelsen deltar på denne evalueringen.

Det sendes også ut en rapport fra virksomhetsanalysen og øvelsen i etterkant, deri også tilbakemelding fra spillstab.

# Referanser

Ebrahimian, A., Esmaeili, S.-M., Seidabadi, A., & Fakhr-Movahedi, A. (2021). The Effect of Psychological Hotwash on Resilience of Emergency Medical Services Personnel. *Emergency Medicine International*, *2021*, 1–7. https://doi.org/10.1155/2021/4392996

Østby, G. (2023). *Digital transformation of public security-developing triple-loop-learning artifacts to meet emerged information security incident response resilience and readiness challenges in public emergency organizations*. https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/3062985

Østby, G. ;, Berg, L. ;, Kianpour, M. ;, Katt, B. ;, & Kowalski, S. (2019). *A Socio-Technical Framework to Improve cyber security training: A Work in Progress*. https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2624957

Østby, G., & Katt, B. (2019). Cyber Crisis Management Roles – A Municipality Responsibility Case Study. In *Science and Technology in Disaster Risk Reduction in Asia* (pp. 168–181). https://doi.org/10.1016/b978-0-12-812711-7.00014-6

Østby, G., & Kowalski, S. J. (2020). Preparing for Cyber Crisis Management Exercises. *N: Schmorrow D., Fidopiastis C. (Eds) Augmented Cognition. Human Cognition and Behavior. HCII 2020. Lecture Notes in Computer Science, Vol 12197.*, 279–290. https://doi.org/https://doi.org/10.1007/978-3-030-50439-7\_19

Østby, G., Lovell, K. N., & Katt, B. (2019). EXCON teams in cyber security training. *Proceedings - 6th Annual Conference on Computational Science and Computational Intelligence, CSCI 2019*, 14–19. https://doi.org/10.1109/CSCI49370.2019.00010

Vykopal, J., Ošlejšek, R., Burská, K., & Zákopčanová, K. (2018). Timely feedback in unstructured cybersecurity exercises. *SIGCSE 2018 - Proceedings of the 49th ACM Technical Symposium on Computer Science Education*, *2018-Janua*, 173–178. https://doi.org/10.1145/3159450.3159561