



Øvelser for bedre
informasjonssikkerhet
(«øvingsspakkene»)

29. oktober 2020
Anders Gundersen

Samarbeidsprosjekt – oppfølging av anbefalinger i DIFI-rapport 2018:4

Analyser av...

- Styring og kontroll (internkontroll)
- Risikostyring
- Beredskap, øvelser og hendelseshåndtering
- Nasjonale felleskomponenter
- Sikkerhetskompetanse
- Sikkerhetskultur
- Etatsstyring



Prioriterte områder:

- Etatsstyring
- Sikkerhetskultur
- Kompetanse
- Øvelser
- Risiko

Organisering

- Prosjektet slått sammen med Digital 2020
- FoU-midler fra JD med bestilling på en digital løsning
- Nye aktører inn i prosjektet



Digitaliseringsdirektoratet
Norwegian Digitalisation Agency



Prosjektleveranse («bestilling»)

- **Utvikle fire enkle øvingskonsept (...og vi har laget 12)**
- Basert på DSBs metodehefter for øvingsplanlegging
- Klart til bruk
 - «Ferdig planlagt»
 - Gjennomføring
 - Evaluering / hvordan evaluere
 - Veien videre
- Digitalt publisert



Omfang / avgrensning

- Små og enkle øvelser (diskusjonsøvelser)
- Spesifikke øvelser for det tekniske miljøet omfattes ikke av dette oppdraget
- Øvelsene skal treffe organisasjonen (ikke eksplisitt IT miljøene)
- Koordineres med planlegging av Digital 2020
- Leveranser skal være tilgjengelig for Nasjonal sikkerhetsmåned
- Vi forholder oss kun til ugradert materiale / tankegods

Mål

«Målet er å gjøre virksomhetene mer beredt til å håndtere informasjonssikkerhetshendelser ved å gi virksomhetene bedre verktøy for å øve på slike hendelser.»

Målgrupper

- Departementer
- Direktoratater
- Fylkesmenn
- Kommuner
- Store bedrifter
- Små og mellomstore bedrifter
- Organisasjoner

«NASJONEN SKAL ØVES»

Hvor lenge siden er det siden din virksomhet øvet på noe som kan være sårbart for organisasjonen?

- 1) Mindre enn en måned
- 2) Mindre enn ett år
- 3) Husker ikke – i tilfelle svært lenge siden...

...og er det nå slik at øvelse gjør mester?

Tja... - det kommer an på...

Suksesskriterier



*«Noen påstår at vi ikke lærer
nok av øvelser, det er de samme
læringspunktene som går igjen»*

Velkommen til øvelser for bedre digital sikkerhet

Velkommen til myndighetenes øvingsportal som skal bidra til at alle virksomheter i Norge får et øvingstilbud innen digital sikkerhet. Bruk av øvelser er sentralt element i Nasjonal strategi for digital sikkerhet.

Portalen er laget som et ledd i den nasjonale øvelsen Digital 2020, og her tilbys diskusjonsøvelser basert på ulike scenarier som kan ramme din virksomhet.


Hensikten med øvelsene er at din virksomhet skal få mulighet til å diskutere seg frem til hvordan det er naturlig å håndtere ulike type hendelser. Samtidig får virksomheten din litt støtte på veien i form av læringsspørsmål som skal gi deg noen hint om hva du uansett bør tenke på og gjøre for å forberede deg på denne type scenarier.


Lykke til!


[Logg inn](#)


[Registrer deg](#)



Hva er en diskusjonsøvelse? 

Kom i gang 

Forskning og diskusjonsøvelser 

Anbefalinger innenfor informasjonssikkerhet 

Scenarier

- Innsidere - vitende
- Innsidere - uvitende
- Kompromitterte servere
- Sårbarhetsvarsling
- Personopplysninger på avveie - forsendelse med epost
- Personopplysninger på avveie - phishing epost
- Personopplysninger på avveie – outsourcet IT-drift og bruk av Office 365
- Hjemmekontor
- Bevissthet rundt egen teknologi på reise/privat
- Direktørsvindel
- Samfunnskritiske funksjoner ute av spill - nettbanker og betalingsterminaler svikter
- Samfunnskritiske systemer ute av spill - strøm slåes ut

Øvelser

Innsider vitende

Scenariot i denne diskusjonsøvelsen handler om hvordan en ansatt deler sensitive organisasjonsinterne opplysninger til tilfeldige nye samarbeidspartnere. Øvelsen gir grunnlag for å diskutere hvordan slike og liknende innsider-trusler kan og bør håndteres.

Sektor: Offentlig

Størrelse: 100+

[Se øvelse →](#)

Samfunnsviktige systemer ute av spill

Scenariet i øvelsen handler om at noen av energisektorens SCADA-systemer blir satt ut av spill og hvilke konsekvenser dette får for din organisasjon. SCADA (Supervisory Control And Data Acquisition) brukes til overvåkning og kontroll av infrastruktur. Det kan også være for eksempel trafikksignaler, gasslinjer, vannverk, eller lufttransport. I løpet av øvelsen kan man gjerne diskutere konsekvenser av bortfall av disse systemene også.

Det er smart å ha med en som jobber med informasjonssikkerhet i øvelsen, for å få vite hva som er situasjonen i din organisasjon i dag. Dersom du ikke har en informasjonssikkerhetsansvarlig i organisasjonen, så er spørsmålene som driver øvelsen fremover (som beskrevet i info til øvingsleder) gode å ha.

Sektor: Offentlig

Størrelse: 100+

[Se øvelse →](#)

Sårbarhetsvarsling

Scenariot i denne diskusjonsøvelsen handler om hvordan organisasjonen kan få sårbarhetsvarsel fra utenforstående hackere. Det vil si at de gir informasjon om at de har funnet sikkerhetshull i organisasjonens systemer.

Sektor: Offentlig

Størrelse: 100+

[Se øvelse →](#)

Personopplysninger på avveie - Phishing

Scenariot i denne diskusjonsøvelsen handler om deling og lagring av informasjon, og hvordan crackere med uedle hensikter kan få tak i informasjonen ved det man kaller «phishing».

Sektor: Offentlig

Størrelse: 100+

[Se øvelse →](#)



Introduksjon til øvelsen

Publisert 13.10.2020

[Informasjon til øvingsleder](#)

Du har nå kommet inn på diskusjonsøvelsen Hjemmekontor.

I lenken øverst på denne siden ligger det litt informasjon til øvingsleder om denne type scenario spesielt, samt noen gode spørsmål spesifikt for dette scenarioet, som øvingsleder kan benytte for å drive diskusjonen fremover. Vi anbefaler øvingsleder å forberede de mest relevante spørsmålene for sin organisasjon.

Etter at du har lest denne introduksjonen vil du komme rett inn på beskrivelse av scenarioet – «Bakgrunnstepe og introduksjon til scenarioet». Dette er en beskrivelse av en gitt hendelse, som kanskje kunne oppstått i din organisasjon, og det er nettopp det vi ønsker dere skal diskutere. Kan dette skje i din organisasjon, hvordan vil dere håndtere en slik situasjon, og hvilke planer har dere for at dette ikke skal skje? På de neste sidene vil det være en utvikling i scenarioet, og innimellom vil dere bli presentert for relevante diskusjonsspørsmål og gode råd om informasjonssikkerhet.

Når dere nå starter opp med øvelsen, så er det altså 8 trinn dere møter:

- 1) Bakgrunnstepe og innledende scenario
- 2) Diskusjonsspørsmål del 1
- 3) Gode råd til videre arbeid del 1
- 4) Scenario del 2
- 5) Diskusjonsspørsmål del 2
- 6) Gode råd til videre arbeid del 2
- 7) Scenario del 3
- 8) Avsluttende informasjon og evalueringsundersøkelse

Lykke til med diskusjonsøvelsen!

Tilbake

Start øvelse

Øvelse i 8 trinn

- 1) Bakgrunnsteppe og innledende scenario
- 2) Diskusjonsspørsmål del 1
- 3) Gode råd til videre arbeid del 1
- 4) Scenario del 2
- 5) Diskusjonsspørsmål del 2
- 6) Gode råd til videre arbeid del 2
- 7) Scenario del 3
- 8) Avsluttende informasjon og evalueringsundersøkelse

Bakgrunnsteppe og Innledende scenario

På denne siden blir du ledet inn i scenarioet. Les gjerne opp teksten for hele gruppen, slik at alle har samme situasjonsforståelse før dere går i gang med diskusjonen.

Bakgrunnsteppe

ABC er en mellomstor organisasjon som tilbyr spesifikke tjenester til private bedrifter og offentlige aktører. De har hovedkontoret sitt like utenfor en større by i Norge.

Selskapet har vokst over tid og ved hovedkontoret er det 48 kontorplasser og 64 ansatte. Mange av kontorplassene er i åpent landskap, og det kan til tider være både støy og uroligheter.

Ledelsen i ABC har en bevisst strategi om manglende kontorplasser, og har blant annet etablert gode løsninger for bruk av hjemmekontor. Flere medarbeidere jobber hjemmefra på egen jobb-PC via privat internett. ABC har i utgangspunktet gode sikkerhetssystemer i form av oppdaterte fjernaksess-løsninger, oppdatert programvare, og sikkerhetsrutiner hos den enkelte medarbeider for bruk av jobb-PC utenfor hovedkontoret.

Organisasjonen ABC er i et marked med stor konkurranse der vurderinger av økonomi og kostnader hele tiden er på agendaen. Kostnader til stadig nye tekniske løsninger og oppgraderinger må justeres og tilpasses etter varierende inntekter og stramme budsjetter. Gode tjenester, kvalitet, pris og omdømme er viktige faktorer for at ABC skal klare seg i det tøffe markedet, noe ledelsen i ABC stadig har fokus på.

Innledende scenario

Birger er en betrodd og erfaren medarbeider i ABC. Han arbeider mye med interne dokumenter, og noen av disse inneholder sensitiv informasjon. Birger benytter seg jevnlig av løsningen med hjemmekontor. Han passer på at fredagen ryddes for møter og reiseorganisasjon, og benytter seg ofte av hjemmekontorløsningen ved ukeslutt. Birger har et eget kontor mellom soverommene til tvillingene Marcus og Martinus, som for tiden går andre året på videregående skole med studiespesialisering innen VK2 Datateknologi og elektronikk.

Diskusjonsspørsmål del 1

På denne siden finner dere noen aktuelle spørsmål for å få i gang diskusjonen.

Har organisasjonen gjort vurderinger i forhold til et slikt scenario tidligere?

Hvilke andre vinklinger av scenarioet kan det være aktuelt å diskutere?

Hvordan kan dere benytte organisasjonens beredskapsplan?

Hvordan kan dere benytte tidligere risikovurderinger organisasjonen har gjort?

Hvordan leverer organisasjonen sine avtaleforpliktelser under disse omstendighetene?

Hvordan leverer organisasjonens systemleverandører sine avtaleforpliktelser under disse omstendighetene?

Ytterligere relevante spørsmål for nettopp dette scenarioet ligger under informasjon til øvingsleder.

På neste side vil dere finne noen gode råd å ta med seg i det videre arbeidet, men vi anbefaler å vente med å gå videre til neste side til alle har fått tatt del i diskusjonen.



Tilbake

Fortsett

Gode råd del 1

På denne siden foreslår vi noen råd for det videre arbeidet med informasjonssikkerhet. Disse rådene er ikke uttømmende, men er i noen grad grunnleggende for arbeidet med informasjonssikkerhet.

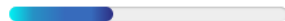
Gjør en god risikoanalyse av organisasjonens behov for beskyttelse av informasjon. Ta utgangspunkt i senarioet, og vurder både konsekvenser og årsaker til at senarioet oppsto. Bruk gjerne tilgjengelige veiledere på hvordan man utarbeider slike risikoanalyser, både for scenarier generelt og for informasjonssikkerhet spesielt.

Lag en god beredskapsplan basert på risikoanalysen. Lag en plan for hvordan organisasjonen ønsker å håndtere et slikt scenario, og for hvem som får ansvar for å gjøre hva.

Gjør en gjennomgang av avtaler med samarbeidspartnere man utveksler informasjon med, for å sjekke ut samarbeidspartneres rutiner for sikring av informasjon.

Gjør en gjennomgang av avtaler med systemleverandør (intern eller ekstern), for å sjekke ut hvordan systemleverandør håndterer slike scenarier, og hvordan de eventuelt eskalerer hendelser dere ønsker å være involvert i.

På neste side blir dere nå ledet inn i andre del av senarioet. Start gjerne med en åpen diskusjon før dere finner frem diskusjonsspørsmålene.



Tilbake

Fortsett

Avsluttende informasjon

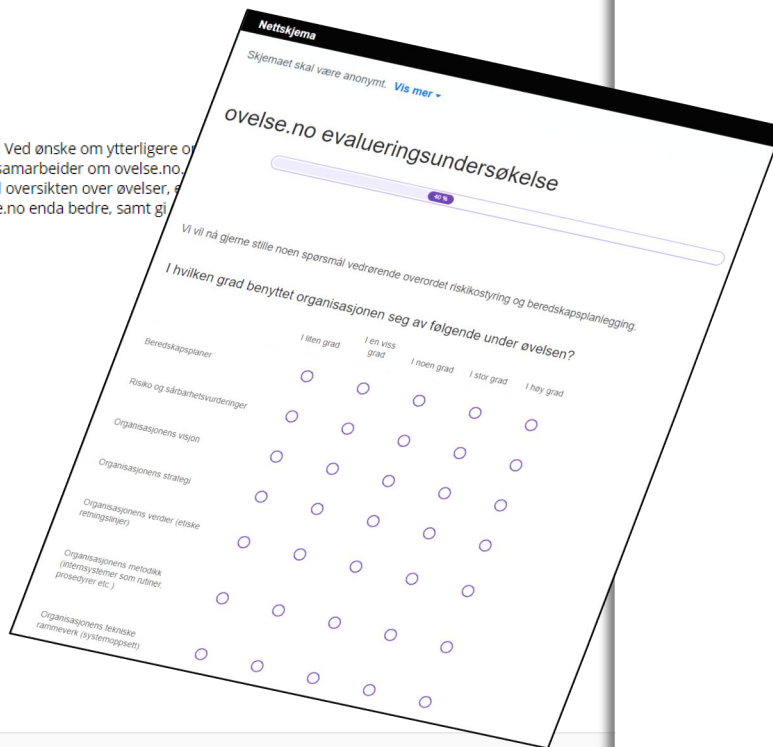
Vi håper dere nå har hatt noen spennende og oppklarende diskusjoner. Ved ønske om ytterligere informasjon om tilbud på web-sidene til de ulike organisasjonene som samarbeider om ovelse.no. Nederst på denne siden kan du nå velge å avslutte øvelsen, gå tilbake til oversikten over øvelser, eller evaluere øvelsen. Evalueringsundersøkelsen vil gi oss verdifullt underlag for å gjøre ovelse.no enda bedre, samt gi oss informasjon om hvordan øvelsene fungerer. Vi håper det kan settes av tid til dette. Vel gjennomført, og lykke til med nye øvelser.



Tilbake

Spørreundersøkelse

Tilbake til øvelseoversikt



Samarbeidspartnere

Ta i bruk!

Informasjonssikkerhet og digitale sårbarheter angår oss alle

Er du knyttet til en offentlig eller privat virksomhet, stor eller liten, eller kanskje du har en rolle i en frivillig organisasjon? Vi har et tilbud om at nettopp din virksomhet på en enkel måte kan øve på en rekke scenarier som handler om informasjonssikkerhet.

På nettsiden www.ovelse.no finner du diskusjonsøvelser tilpasset nettopp din organisasjon. De er klare til å tas i bruk, og du trenger ingen spesiell kompetanse for å lede en slik diskusjonsøvelse.

Hensikten og målsettingen med å lage slike øvelser er å øke bevisstheten omkring digitale sårbarheter og gjøre samfunnet bedre forberedt på å håndtere uønskede digitale hendelser.

Øvelsene skal treffe organisasjonen, både ledelse og fagmiljø, og ikke nødvendigvis bare IKT-miljøene. Det er derfor utarbeidet tolv

diskusjonsøvelser (øvingspakker) innen digital sikkerhet og beredskap.

Hver øvelse inneholder et aktuelt scenario med tilhørende læringspørsmål. Det er ingen fasit bevisstgjørende diskusjon.

Øvelsene finner du på www.ovelse.no og det koster ikke noe å benytte disse.

Ta øvingspakkene i bruk, og husk at dette skal være en øvelse og ikke en prøvelse.



www.ovelse.no