# Intervjuguide

# Håndtering av IKT-sikkerhetsbrudd

Cathrine Hove, Marte Tårnes

Vi skal kartlegge hvordan IKT-sikkerhetsbrudd håndteres i virksomheter. Vi ønsker å finne ut hva slags planer som eksisterer, i hvilken grad disse planene er basert på standarder, i hvilken grad de blir fulgt i praksis og om det har fungert bra. Datainnsamlingen vil, i tillegg til en bakgrunnsstudie om hendelseshåndtering, danne grunnlaget for en masteroppgave.

Intervjuene vil bli gjennomført ansikt til ansikt i full fortrolighet og alle svar anonymiseres. Resultatene vil ikke kunne spores til enkeltindivider eller enkeltvirksomheter.

## Innledning

**Hvem vi er:**

Masterstudenter i kommunikasjonsteknologi med fordypning informasjonssikkerhet.

**Kontekst:**

Masteroppgave

**Forskningsspørsmål:**

- Hvordan utfører virksomheter hendelseshåndtering i praksis?

Med underspørsmålene:

- Hvilke planer og prosedyrer for hendelseshåndtering er etablert i virksomheter?
- Til hvilken grad blir eksisterende standarder/retningslinjer brukt i planer for hendelseshåndtering?
- Hvordan har tidligere hendelser blitt håndtert i henhold til forhåndsbestemte planer?

**Meldeplikt:**

Vi kommer til å bruke båndopptaker og derfor er studien meldt til Personvernombudet for forskning, Norsk samfunnsvitenskapelige datatjeneste (NSD). Informasjon til intervjuobjektene finnes i eget informasjonsskriv sammen med en samtykkeerklæring.

**Formalia:**

Tidsramme: mellom en og to timer

Vi bruker båndopptaker.

Vi har en intervjuguide som følges løst og vi ønsker å få til en samtale rundt temaet.

## Spørsmål

Spørsmålene er nummererte med potensielle underspørsmål. Hva slags spørsmål som faktisk stilles kan variere etter f.eks. hvilken rolle intervjuobjektet/intervjuobjektene har i virksomheten og hva slags type virksomhet det er (f.eks. om de drifter systemer for andre).

**Innledende:**

1. Hvor mange ansatte er dere i virksomheten?
2. Hva slags type organisasjon er dette/hva er kjernevirksomheten deres?
3. Hva er din/deres rolle i virksomheten?
    a. Hvor lenge har du hatt denne rollen?
4. Hvordan er IT-driften deres organisert?

**Generelt:**

5. Hvordan definerer du et IKT-sikkerhetsbrudd?
    a. Er denne definisjonen noe som virksomheten har utviklet og som er kjent blant ansatte?
6. Hva er det verst tenkelige sikkerhetsbruddet dere kan oppleve?
    a. Hva slags konsekvenser kan et eventuelt slikt brudd få?
7. Har dere en oversikt over tidligere sikkerhetsbrudd?
8. Har dere en sikkerhetspolicy?
9. Har dere en egen policy for hendelses-/sårbarhetshåndtering?

**Incident Response Team:**

10. Har dere noe dedikert team for hendelseshåndtering (CIRT/CSIRT/ISIRT/IRT)?
    a. Hvordan er teamet organisert?
        i. Hvem er med?
        ii. Hvordan ble de valgt?
        iii. Er teamet internt eller helt/delvis outsourced?
        iv. Er teamet sentralt eller distribuert?
        v. Jobber medlemmene heltid eller deltid i teamet?
        vi. Hvordan er tilgjengeligheten på medlemmene?
        vii. Hvordan er roller og ansvar i teamet organisert?
    b. Inngår forebyggende arbeid som en del av teamets oppgaver, dvs. sikring av nettverk, systemer osv.?
        i. Holdningsskapende arbeid?
        ii. Har de andre oppgaver?
    c. Hvordan er samarbeidet/kommunikasjonen mellom teamet og
        i. Ledelsen?
        ii. CISO/CIO og IT-sjef?
        iii. Kriseteam?
        iv. Andre team?
    d. Hvilken opplæring har teamet gjennomgått?

        i. Ekstern?
        ii. Intern?
        iii. Får de kontinuerlig opplæring?
11. Hvilken nytte kan dere se/har dere sett av å ha et slikt team?

**Planlegging/forberedelse:**

12. Finnes det en *helhetlig* (altomfattende) plan for håndtering av sikkerhetsbrudd?
    a. Brukes den i praksis?
    b. Er denne koordinert med eventuelle kunder som dere drifter systemene for?
13. Hvilke planer for kommunikasjon eksisterer?
    a. Hvem skal/kan kontaktes i ulike tilfeller?
    b. Hvordan håndteres kontakt med "outsiders" (media, politi, operatører osv.)?
14. Har dere en spesifisert work flow for hendelseshåndteringsprosessen?
    a. Hvordan er den utarbeidet og vedlikeholdt?
    c. Hvordan blir den kommunisert til medlemmene i hendelseshåndteringsteamet?
    d. Hvordan har denne fungert i praksis/har den blitt fulgt?

**Standarder:**

15. Følger dere ISO/IEC 27001/27002?
    a. Er dere sertifisert?
    b. Hvordan oppfyller dere kravene som omhandler hendelseshåndtering? (Gå gjennom standard, steg for steg)
16. Følger dere noen standarder eller guidelines som spesifikt omfatter hendelseshåndtering?
    a. Hvilke?
    b. Bruker dere ISO/IEC 27035 (tidligere ISO/IEC 18044)?
        i. Har dere hørt om den?
    c. Hvordan har dere tilpasset guider til deres organisasjon ut fra standardene?
    d. Hvorfor ikke?
        i. Har dere vurdert det?
17. Når begynte dere å følge standarder?
    a. Hvilken innvirkning har det hatt på hendelseshåndteringen?
18. Brukes en standard/guide for kategorisering av hendelser, basert på
    a. Alvorlighetsgrad?
    b. Type?

**Rutiner:**

19. Hva slags rutiner har dere for varsling av potensielle sikkerhetsbrudd?
    a. Hvordan blir de ansatte informert om disse rutinene?
    b. Hvilke rutiner for varsling finnes hos kunder dere drifter for?
    c. Kan sårbarheter varsles på samme måte?
    d. Hvordan håndteres konfidensiell informasjon ved varsling om sikkerhetsbrudd?
        i. Blir anonymitet for de som varsler om hendelser ivaretatt?
    e. Hvem mottar varslene og avgjør hva som skal skje videre?
20. Har dere noen form for sjekkliste for bruk ved hendelseshåndtering?
    a. Har dere laget den selv?
        i. Hvis nei, hvor kommer den fra?

21. Hvordan håndterer dere sårbarheter som blir oppdaget (som enda ikke er utnyttet)?
22. Hva slags rutiner har dere for "høynet beredskap" ved hendelser deres eget team ikke har kompetanse til å håndtere eller ressurser til å utføre håndteringen raskt nok?
    a. Utvider dere håndteringsteamet?
    b. Kalles det inn et kriseteam?
        ii. Eksternt?
        iii. Internt?

**Hendelseshåndtering:**

23. Hvordan blir sikkerhetsbrudd vanligvis oppdaget? (automatisert, sluttbruker?)
24. Har dere noen prosedyrer for håndtering av *kjente* sikkerhetsbrudd eller sårbarheter?
    a. Har dere automatisk håndtering av noen typer sikkerhetsbrudd?
25. Finnes det eksempler på hendelser der rutinene/planene har fungert godt?
    a. Hva ble gjort riktig i disse tilfellene?
    b. Ble det dokumentert og delt med eksterne virksomheter?
26. Finnes det eksempler på hendelser der rutinene/planene har fungert dårlig?
    a. Hvorfor fungerte det dårlig?
    b. Ble det dokumentert og delt med eksterne virksomheter?
27. Hvordan sikres digitale bevis i forbindelse med et sikkerhetsbrudd?
28. Før avgjørelser om hvordan hendelser skal håndteres blir tatt, vurderes omfanget og mulige konsekvenser for kjernevirksomheten?
29. Hva gjøres for å sikre at gjenoppretting av systemer etter hendelser skal gå så raskt som mulig?
    a. Hvordan har dette fungert i praksis?

**Dokumentasjon og rapportering:**

30. På hvilken måte dokumenterer dere hendelser?
    a. Er dette en kontinuerlig prosess eller gjøres det f.eks. kun etter endt hendelse?
    b. Har/bruker dere noen mal for rapporter?
31. Hva dokumenteres?
    a. Kostnader?
    b. Type?
    c. Omfang?
    d. Aktiviteter foretatt av involverte personer?
    e. Hendelsesforløpet?
32. Hvordan blir hendelser rapportert til ledelsen?
    a. Hvilke hendelser blir rapportert?
    b. Hvem i ledelsen blir det rapportert til?

**Øvelser:**

33. Utfører dere noen øvelser for å sjekke om planene ser ut til å fungere i praksis?
    a. Kan du forklare litt om hvordan det gjøres?
34. Tilsier erfaring at øvelsene var hensiktsmessige?
35. Har du noen eksempler på forbedringsområder som har blitt avdekket gjennom øvelser?

**Etterarbeid/forbedringspotensiale:**

36. Hvordan samles erfaringer gjort ved ulike hendelser?
    a. Blir erfaring fra alle typer hendelser dokumentert og distribuert?
    b. Hvis ikke, hvorfor det?
37. Hvilke rutiner finnes for å lære av feil (lessons learned)?
    a. Har dere møter etter endt hendelse?
    b. Har dere regelmessige møter?
    c. Kan dere komme på tilfeller hvor dere har brukt "lessons learned" fra en tidligere hendelse for å håndtere en ny hendelse på en bedre måte?
38. Deles erfaring fra enkelthendelser med andre (begge veier)?
    a. Andre virksomheter?
    b. NorCERT?
    c. Andre?