**Intervjuguide**

**Håndtering av IKT-sikkerhetsbrudd**

Cathrine Hove, Marte Tårnes

Vi skal kartlegge hvordan IKT-sikkerhetsbrudd håndteres i store 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, si tillegg til en bakgrunsstudie om hendelseshåndtering, danne grunnlaget for en masteroppgave.

Intervjuene vil bli gjennomført ansikt til ansikt i full fotrolighet 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:**

**Meldeplikt:**

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

**Formalia:**

Tidsramme: ca en time, kanskje lit mer for noen av intervjuene

Vi bruker båndopptaker.

Vi har en intervjuguide som følges løst og 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?
   1. Evt. også hvor mange ansatte det er i virksomheter som bedriften drifter aktuelle systemer for
2. Hva slags type organisasjon er dette/hva er kjernevirksomheten deres?
   1. Evt. samme spørsmål for aktuelle virksomheter som eier systemer som blir driftet av intervjueobjektets bedrift
3. Hva er din/deres rolle i virksomheten?

**Håndtering av sikkerhetsbrudd:**

1. Hvordan definerer du et IKT-sikkerhetsbrudd (incident)?
   1. Er dette en definisjon som virksomheten har satt og som alle vet om?
2. Bruker/følger dere noen standarder eller guides/guidelines som omfatter hendelseshåndtering?
   1. Hvilke?
   2. Bruker dere ISO/IEC 27035?
      1. Er dere sertifisert?
   3. Bruker dere NIST SP 800-61?
   4. Hvorfor ikke?
   5. Har dere vurdert det?
3. Har dere noe CIRT (Computer Incident Response Team)/ISIRT (Information Security Incident Response Team)?
   1. Hvem er med? (hvordan ble de valgt?)
   2. Hvordan er tilgjengeligheten på medlemmene(24/7)?
   3. Inngår preparation som en del av teamets arbeid, i.e. sikring av nettverk, systemer osv.?
   4. Håndterer de beredskapsplanlegging?
   5. Hvis nei: Hvem er ansvarlig dersom det skjer en hendelse?
4. Utfører dere noen øvelser for å sjekke om ansatte vet hvordan de skal håndtere ulike hendelser?
   1. Kan du forklare litt om hvordan det gjøres?
5. Hva slags rutiner har dere for rapportering av hendelser (når noen mistenker at noe har skjedd)?
   1. Hvordan blir de ansatte informert om disse rutinene? Vet de hva de skal gjøre?
6. Har dere noen form for “Incident Handlers Checklist”?
   1. Har dere laget den selv?
   2. Hvis nei, hvor kommer den fra?
7. Har noen i virksomheten gjennomgått noe “training” i forhold til incident respons?
   1. Hvilken?
   2. Hvem?
8. På hvilken måte dokumenterer dere hendelser?
   1. Har dere noen mal for rapporter av hendelser?
   2. Har dere noe Incident Tracking System?
9. Hvordan håndterer dere sårbarheter (vulnerabilities) som blir oppdaget (som enda ikke er utnyttet)?
   1. Hva slags rapporteringssystem har dere for sårbarheter?
10. Eksisterer det en oversikt/plan for kommunikasjon? Hvem skal/kan kontaktes i ulike tilfeller? Hvordan er kontakten med “outsiders” (media, politi, operatører osv.)? Blir riktig informasjon gitt til riktige personer?
11. Finnes det en *helhetlig* (altomfattende) plan (approach) for håndtering av sikkerhetsbrudd (eller eksisterer det planer, men nødvendigvis ikke en overordnet systematisk plan)?
    1. Er denne koordinert med eventuelle kunder som dere drifter systemene for? Vet de hva de skal gjøre hvis de oppdager noe mistenkelig? Ser de etter det i det hele tatt?
12. Har dere kategorisering og prioritering av hendelser? Alvorlighetsgrad? Håndteres de forskjellig? Brukes en standard for kategoriseringen av alvorlighetsgrad?
13. Finnes det eksempler på hendelser der rutinene/planene har fungert godt? Hva ble gjort riktig i disse tilfellene? Ble det dokumentert og delt med team i andre bedrifter?
14. Hvordan samles erfaringer gjort ved ulike hendelser? Finnes det standardiserte gjennomganger for å “lære av feil”? (lessons learned). Det kan være forskjell på “high-impact” og “high learning” incidents. Blir erfaring fra alle typer hendelser dokumentert og distribuert?
    1. 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?
    2. Blir erfaring fra enkelthendelser delt med andre(bedrifter)?
15. Hva er det verst tenkelige sikkerhetsbruddet dere kan oppleve?
    1. Hva slags konsekvenser kan et eventuelt slikt brudd få?
16. Har dere en database med tidligere sikkerhetsbrudd?
17. Har dere noen prosedyrer for håndtering av kjente sikkerhetsbrudd, sårbarheter eller hendelser?
    1. Har dere noen automatisk håndtering av noen typer hendelser/sikkerhetsbrudd?
18. Blir anonymitet for de som varsler om hendelser ivaretatt?
19. Hvordan håndteres konfidensiell informasjon ved rapportering om sikkerhetshendelser(brudd)?
20. Hvilke tiltak har fungert og hvordan har evalueringen av virkningen av tiltakene vært? (aksjonsforskning).