Universitetet i Oslo
IN2120 Informasjonssikkerhet
Høst 2018
Workshop-spørsmål

Forelesning 6: Hendelsesrespons og digital etterforskning

Spørsmål 1

a. Vanlige ansatte er ofte viktige når det gjelder å oppdage sikkerhetshendelser. Hvilke verktøy har en organisasjon for å sikre at de ansatte rapporterer mulige hendelser?
b. Hva er de viktigste elementene i en policy for hendelsesrespons?
c. Beskriv de 3 hovedtyper av responsteam.

Spørsmål 2

Følgende er trinn i hendelsedresponsprosessen. Forklar kort hvert trinn.
a. Deteksjon
b. Sortering
c. Innsamling
d. Skadebegrensning
e. Analyse og etterforskning
f. Rapportering
g. Gjenoppretting

Spørsmål 3

Bevismaterialets integritet er avgjørende for at det skal kunne brukes i retten og ha tyngde.
a. Hva er *notoritet* og hvorfor er det viktig for bevismaterialets integritet?
b. Forutsatt at de som foretar digital etterforskning følger de riktige trinnene for å bevare bevismaterialets integritet og notoritet, hva må de gjøre for å overbevise retten om at de faktisk har gjort det?

Spørsmål 4

Forklar trinnene i prosessen for digital etterforskning.

Spørsmål 5

a. Forklar forskjellen mellom «live» innsamling og «post mortem» innsamling?
b. Hva er fordelene og ulempene ved «live» og «post mortem» innsamling?
c. Gi et eksempel når «Live» innsamling er nødvendig.

Spørsmål 6

Forklar de grunnleggende prinsippene i etterforskningsprosessen.