IN1020: Øvingsoppgaver undervisningsuke 2 (2-6. september 2019)

Oppgave 1 Hva er forskjellen på punkt-til-punkt nettverk og et broadcast nettverk?

Oppgave 2 Hvorfor er nettverket organisert i lag?

Oppgave 3

a) Hvilke lag finner vi vanligvis i Internett?

b) Hva er oppgaven til hvert av de forskjellige lagene?

Oppgave 4 Hvorfor ønsker man at brukere av et trådløst nett (f.eks. UiO-nettet/eduroam) skal autentisere seg før de får tilgang til nett og ressurser i nettet?

Oppgave 5: Behandling av data

Gjør en vurdering av hvordan du lagrer og behandler egne data/informasjon. Private, på UiO/Ifi, jobb. Ta utgangspunkt i mulige sikkerhetstrusler og sikkerhetstiltak du allerede har eller bør iverksette, og kikk gjerne på UiOs veiledning for klassifisering av data ((https://www.uio.no/tjenester/it/sikkerhet/lsis/tillegg/infoklasser.html). og Lagringsguide ((https://www.uio.no/tjenester/it/sikkerhet/lsis/tillegg/lagringsguide.html)).

Oppgave 6: Tilgangskontroll

a) En vanlig misforståelse er å blande begrepene autorisasjon (authorization) og tilgangskontroll (access control). Repeter og vær sikker på at du forstår forskjellen.

b) Tilgangskontroll i Devilry: I innleveringssystemet Devilry som vi bruker på Institutt for informatikk har en bruker ulike roller i ulike emner: Student, retter, faglærer og administrator (typisk studieadministrasjonen). Studenter leverer oppgaver, rettere retter og gir tilbakemeldinger på oppgaver, faglærer legger til rette for innlevering og administratorer har full oversikt over absolutt all informasjon i stystemet.

Etter mal fra forelesning: Tenkt deg fram til og gi eksempler på subjekt, objekt og handling i systemet Devilry. Ikke bind deg til handlinger du tror er tillatt!

Oppgave 7: Datalekkasjer

Datalekkasjer skjer ofte. https://haveibeenpwned.com/PwnedWebsites er en nettside med oversikt over de fleste store datalekkasjer, og vi kan se at f.eks. kjente, store virksomheter som Adobe og linkedin har hatt datalekkasjer der både brukernavn og passord er lekket. https://haveibeenpwned.com/ er en ideell virksomhet som drives av anerkjente aktører, men være likevel varsom med å oppgi informasjon om deg selv på denne typen nettsider. Oppgi **aldri** en gyldig kombinasjon av brukernavn og passord til ukjente nettsteder!

a) På https://haveibeenpwned.com/Passwords kan du sjekke om et passord figurerer på lister over passord som har lekket. Test vanlige passord som 1234546 og qwerty. Vær skeptisk til å skrive inn og teste passord du har i bruk, du vet lite om sikkerheten i tjenesten.

b) Undersøk hvilke datalekkasjer adressen kritisk@ifi.uio.no figurerer i på https://haveibeenpwned.com/