Informasjonssikkerhet: Teori og praksis

Audun Jøsang
2. utgave 2023
Universitetsforlaget

Oppgaver

Kapittel 15: Regelverk for informasjonssikkerhet

Oppgave 1. Ansvar

Se for deg at selskap A og selskap B av samme størrelse blir ofre for cyberangrep, og at begge selskapene får betydelige tap som negativt påvirker kunder og aksjonærer. Begge selskap er underlagt lovkrav om å ha et styringssystem for informasjonssikkerhet. Under etterforskning av hendelsene blir det funnet at selskap A har implementert et ISMS (styringssystem for informasjonssikkerhet) og har god modenhet for ledelse av informasjonssikkerhet, mens selskap B har mangelfullt ISMS og bare har en ad hoc ledelse av informasjonssikkerhet. Hvis man antar at tapet for begge selskapene er i samme størrelsesorden, forklar mulige forskjeller mellom selskapene vedrørende reaksjoner og sanksjoner mot selskapene eller deres ledelse.

Oppgave 2. Kraftberedskapsforskriften

Selskapet Sky-Kraft (et fiktivt selskap) ønsker å tilby skybaserte IoT-løsninger for bryterfunksjonalitet i kraftforsyningen, f.eks. for måling av elektrisk energi og begrensning av energi- og effektuttaket ved det enkelte målepunkt. Tjenestene skal la kraftselskapene utføre bryterfunksjonalitet fra enkle brukerterminaler gjennom Internett fra hele verden. Sikkerhet skal ivaretas bl.a. med sterk 2-faktorautentisering med BankID.

Vil en slik løsning være lovlig i henhold til Kraftberedskapsforskriften?
Forklar hvorfor / hvorfor ikke.

Oppgave 3: Regelverk fra EU

Direktiver (directives) og forordninger (regulations) er ulike regelverk (acts) som utvikles og publiseres av EU. Som EØS-land gjelder mange av disse for Norge.

a. Hvordan bestemmes det om et direktiv eller forordning skal gjelde for Norge?
b. Hva er et EU-direktiv, og hvordan implementeres et EU-direktiv i Norge?
c. Hva er en EU-forordning, og hvordan implementeres en EU-forordning i Norge?

Oppgave 4: NIS2-direktivet

a. Hva står forkortelsen NIS for?
b. Hva er hovedformålet med EUs NIS2-direktiv?
c. Hvordan planlegger Norge å implementere NIS2-direktivet?

Oppgave 5: Sammenheng mellom forskrifter og lover

a. Lover og forskrifter er ulike typer regelverk, se s.4 i forelesningspresentasjon del 3.a. Hvordan er lover og forskrifter relatert?
b. Hvordan finner man lovhjemmel til en forskrift?
c. Finn lovhjemler for
   - Virksomhetssikkerhetsforskriften
   - Kraftberedskapsforskriften
   - Forskrift om IT-standarder i offentlig forvaltning
d. Hva betyr begrepet forvaltningsmyndighet?
e. Finn hvem som forvalter
   - Sikkerhetsloven
   - Kraftberedskapsforskriften
   - Forvaltningsloven
f. Finn hvem som er underlagt
   - Sikkerhetsloven
   - Kraftberedskapsforskriften
   - Forvaltningsloven
g. Finn kapitler/paragrafer som omhandler informasjonssikkerhet i
   - Sikkerhetsloven
   - Kraftforsyningsforskriften
   - Forskrift om IT-standarder i offentlig forvaltning

Oppgave 6: Sikkerhetsloven

a. Beskriv kort sikkerhetslovens formål (§ 1-1. Formål). Beskrivelsen trenger ikke være ordrett samme tekst som i loven.
b. Nevn hvilken type årsak/kilde til sikkerhetshendelser som er fokus for sikkerhetsloven.
c. Hvorfor kunne ikke sikkerhetsloven danne grunnlag for å tilpasse EUs NIS2-direktiv?