Universitetet i Oslo
IN2120 Informasjonssikkerhet
Høst 2023
Teoretiske oppgaver

Del 11: Sikkerhetskultur og sikkerhetsledelse

Oppgave 1: Bygging av sikkerhetskultur

a. Ta utgangspunkt i dimensjonene for sikkerhetskultur beskrevet i avsnitt 13.1 i læreboka. Nevn eksempler på dårlig sikkerhetskultur for de forskjellige dimensjonene.
b. Med utgangspunkt i eksemplene fra a: Foreslå tiltak for å forbedre sikkerhetskulturen.
c. Foreslå mulige strategier som er egnet til å styrke kunnskap, motivasjon, holdninger og atferd med hensyn til informasjonssikkerhet for følgende kategorier av ansatte i en organisasjon:
   i) motiverte
   ii) likegyldige
   iii) misfornøyde
   iv) hemmelige agenter for fremmede stater

   Hvordan kan ulike strategier anvendes når det er uvisst hvilken kategori hver ansatt passer inn i, eller bør man forsøke å utforme en strategi som passer for alle kategorier av ansatte?

Oppgave 2: Innsidetrusselen

a. I perioden fra å bli ansatt til å slutte i et selskap, når er det størst sannsynlighet for at en ansatt blir en innsidetrussel?
b. Tiltak for å bygge holdninger og personlig integritet kan bidra til å forhindre at anstte blir en innsidetrussel. Hva er en type innsidetrussel som er lite påvirkelig for denne typen tiltak?

Oppgave 3: Sosial manipulering

a. Beskriv måter å bruke sosial manipulering på for
   - å installere skadevare på PC-en til administrerende direktør i et selskap
   - å få uautorisert tilgang til bygningen for selskapets hovedkontor
b. Tenk deg at ansatte utgjør menneskelig «IDS» (Intrusion Detection System) mot sosiale manipuleringsangrep. Hva ville være en «falsk positiv» og en «falsk negativ» deteksjon av sosial manipulering? Vurder potensiell alvorlighet av falsk positiv og falsk negativ deteksjon av sosial manipulering.
c. Hva bør du gjøre hvis du tror du er blitt lurt av sosial manipulering?

Oppgave 4: Case om sikkerhetskultur

Din bedrift er i en sektor som typisk er utsatt for digitale sikkerhetstrusler. Policyer for informasjonssikkerhet fins, men ledelsen har ikke informert ansatte om disse. På pub etter jobben enn dag snakker du og noen kollegaer om informasjonssikkerhet i bedriften. En kollega nevner at når han mottar en phishing-epost, klikker han ofte på lenker og åpner vedlegg for moro skyld. Du syns det er dumt å gjøre, men sier intet fordi du ikke ville kritisere ham. Din kollegas holdning til phishing-eposter gjør deg urolig, så dagen etter snakker du med IT-drift om at en kollega klikker på phishing lenker for moro skyld. Du får til svar at så lenge det ikke har skjedd noe, trenger man ikke være urolig, og du at gjerne kan ta kontakt hvis du tror du er blitt lurt og det faktisk har skjedd noe.

a. Nevn aspekter du mener reflekterer dårlig sikkerhetskultur.
b. Gi forslag til hvordan sikkerhetskulturen kan forbedres, ikke bare ved å endre på de negative aspektene i a), men hvilke generelle tilnærminger for sikkerhetskultur som kan benyttes.

Oppgave 5: ISMS

a. Hvordan er standardene ISO/IEC 27001 og ISO/IEC 27002-relatert?
b. Hva betyr "system" i forkortelsen ISMS (Information Security Management System) (Ledelsessystem for informasjonssikkerhet)?
c. Hvilken av ovennevnte standarder danner grunnlag for sertifisering, og hvorfor?
d. Hvordan bør en organisasjon avgjøre hvilke sikkerhetstiltak som skal implementeres?

Oppgave 6: Kategorisering av informasjonssikkerhetstiltak

Standarder og veiledere som beskriver informasjonssikkerhetstiltak benytter ulike kategoriseringer av sikkerhetstiltakene. Tre vanlige kategoriseringer er:

- Prosesskategorier (kartlegge > beskytte > detektere > respondere > gjenopprette)
- Abstrakte kategorier (organisatoriske, personell, fysiske, og teknologiske tiltak)
- Operasjonelle kategorier (f,eks. tiltak for tilgangskontroll, data/media-beskyttelse, IAM, nettverkssikkerhet, system/applikasjonssikkerhet, hendelsesrespons, opplæring, leverandørsikkerhet etc.)

For hver standard/veileder nedenfor, spesifiser hvilken kategorisering den benytter.

a. ISO/IEC 27002:2022 Information security controls
b. NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations
c. NSMs Grunnprinsipper for IKT-sikkerhet
d. NIST Cyber Security Framework
e. CIS Critical Security Controls