Universitetet i Oslo
IN5080 Sikkerhets- og risikostyring
Vår 2025

Semesteroppgave

Denne oppgaven utgjør midtsemestereksamen i IN5080 2025. Oppgavebesvarelsen blir vurdert som en deleksamen med en skåring i intervallet 0 – 100. Skåringen teller med relativ vekt 0,3 for fastsettelse av karakteren i emnet. Alle i samme gruppe få samme skåring.

Oppgave A: Vurdering av modenheten til UiOs LSIS (teller 20%)

Du jobber i et konsulentselskap som har fått i oppdrag å vurdere modenhet av UiOs styring av informasjonssikkerhet i henhold til CMMI (Capability Maturity Model Integration). En kort beskrivelse av modenhetsnivåene i CMMI ligger på semestersiden:
https://www.uio.no/studier/emner/matnat/ifi/IN5080/v25/forelesningsvideoer/cmmi-for-cybersikkerhet.pdf

Oppgave: Skriv en vurdering med argumenter for hvilket/hvilke CMMI-modenhetsnivå(er) som best reflekterer UiOs modenhetsnivå. Vurderingen skal baseres på UiOs LSIS, og skal referere til spesifikke utsagn fra policyer i UiOs LSIS. Det er mulig at UiOs modenhetsnivå ikke er entydig, men ligger delvis på flere nivåer. Hvis dette er tilfelle, skal det begrunnes.

UiOs LSIS er dokumentert på UiOs nettsider: https://www.uio.no/tjenester/it/sikkerhet/lsis/

LSIS (Ledelsessystem for informasjonssikkerhet) og ISMS (styringssystem for informasjonssikkerhet) har samme betydning.

Oppgave B: Sammenligning av sikkerhetstiltak fra ulike kilder (teller 20%)

Ulike kilder (standarder/veiledere) beskriver typisk de samme sikkerhetstiltakene på litt forskjellige måter. Denne oppgaven fokuserer på sikkerhetstiltaket **8.13 Sikkerhetskopiering av informasjon** fra ISO/IEC 27002, og tilsvarende tiltak beskrevet i andre kilder.
Sikkerhetstiltak 8.13 i ISO/IEC 27002 og tilsvarende tiltak er beskrevet i følgende kilder:

1. ISO/IEC 27002 Sikkerhetstiltak (utdrag)
   https://www.uio.no/studier/emner/matnat/ifi/IN5080/v25/forelesningsvideoer/utdrag-fra-iso-iec-27002.pdf
2. NIST CSF 2.0, se oversikt: https://doi.org/10.6028/NIST.CSWP.29
   Regneark med eksempler og referanser:
   https://csrc.nist.gov/extensions/nudp/services/json/csf/download?olirids=all
3. CSC (Critical Security Controls) fra CIS (Centre for Internet Security):
   https://www.cisecurity.org/controls
4. NSMs grunnprinsipper for IKT-sikkerhet:
   https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet/introduksjon/
5. SP 800-53 Security and Privacy Controls for Systems and Organizations:
   https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

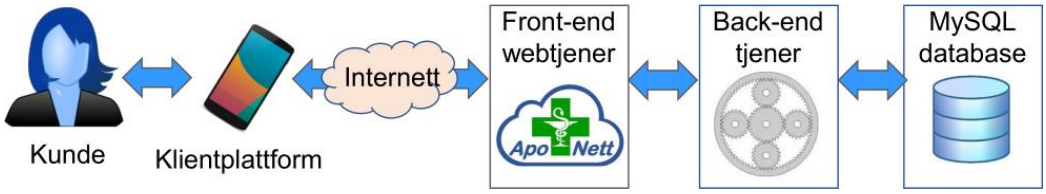
Oppgave:

a. Identifiser og nevn tilsvarende tiltak fra ISO/IEC, NIST CSF, CSC, NSM og SP 800-53. Hvilke begreper bruker kildene 2-5 for begrepet «sikkerhetskopiering» i ISO/IEC 27002?
b. Velg tre (3) relevante/viktige aspekter ved de ulike beskrivelsene av sikkerhetstiltaket «sikkerhetskopiering». Beskriv om, og i hvilken grad hvert aspekt er beskrevet henholdsvis i hver av de fem kildene.

Oppgave C: DPIA og Risikovurdering av

Denne case-oppgaven handler om (det fiktive) firmaet Apo-Nett som skal implementere et nettapotek. Informasjonssikkerhet og personvern er viktige aspekter for å beskytte verdier mot trusler, men designerne av Apo-Nett mangler forståelse for å ta tilstrekkelig hensyn til disse aspektene under spesifiseringen. Anta at du/dere er leid inn som konsulenter for å gjøre risikostyring og vurdering av personvernkonsekvens i den foreslåtte designen av Apo-Nett.

Apo-Nett skal bygges som en PaaS-skyløsning (Platform-as-a-Service). En PaaS-løsning betyr at skyleverandøren hovedsakelig har ansvar for de fysiske maskinene samt operativsystemet (kunden trenger f.eks. ikke å oppdatere OS og database-serveren selv). Hovedelementene i Apo-Nett sin skyløsningen er front-end, back-end og database som vist på Figur 1 nedenfor. Hvis beskrivelsen mangler detaljer som synes nødvendig for å besvare oppgavene, er det helt greit å gjøre antagelser.



Figur 1. Løsning - generell oversikt

Foreslått løsning

Designerne av Apo-Nett ønsker å lage en fleksibel løsning som skal være enkel for kundene og enkel for Apo-Nett å utvikle, drifte og admininstrere. Apo-Nett ønsker å bruke DevOps som tilnærming, dvs. at både utvikling og drift foregår på samme sky-plattform. Alle foreslåtte spesifikasjoner er nummerert nedenfor.

1. Designerne foreslår å la kunde-login foregå på tre alternative måter:
   - Direkte login til Apo-Nett med lokal ID som er et selvdefinert brukernavn, og et selvdefinert passord lagret som klartekst i en passordfil i PaaS-løsningen.
   - Login med Internett-ID, f.eks. epost-adresse med autentisering fra f.eks. facebook, twitter eller google.
   - Login med sterk ID, dvs. fødselsnummer, autentisert med BankID, Commfides, eller Buypass, som gir autentiseringsnivå HØYT ifølge *Veileder for identifikasjon og sporbarhet i elektronisk kommunikasjon med og i offentlig sektor,* fra DigDir.

2. Designerne foreslår at kundedatabasen inneholder følgende:
   - Navn
   - Epostadresse
   - Telefonnummer
   - Kjønn (frivillig)
   - Fødselsdato (frivillig)
   - Lokalt brukernavn og passord i klartekst (for kunder som bruker lokal ID)
   - Internett-ID (for kunder som bruker Internett-ID)
   - Fødselsnummer (for kunder som bruker sterk ID)
   - Kjøpshistorie med alle tidligere kjøpte produkter

For bestilling av vanlige produkter som vitaminer, kan lokal ID ellet Internett-ID benyttes. For bestilling av reseptbelagte produkter kreves sterk ID med fødselsnummer. Designerne ønsker følgende fleksibilitet:

3. En kundekonto opprettes med en av ID-typene, men kan utvides til å også benytte andre ID-typer for samme kunde-konto.

Designerne ønsker følgende alternative løsninger for betaling:

4. Betaling kan gjøres med følgende løsninger:
   - Bankkort/kredittkort, der bank vil be om sterk ID ved betaling. Brukerkontoen i Apo-Nett trenger ikke sterk ID, fordi ID for betaling er uavhengig av kunde-ID.
   - Vipps.

For kunder med Internett-ID, ønsker designerne å knytte Apo-Nett til andre tjenesteleverandører gjennom OAuth-API, som tillater følgende funksjoner:

5. Apo-Nett kan motta info fra andre tjenestetilbydere som f.eks. treningsstudioer slik at Apo-Nett de kan tilby relevante helseprodukter til kunder i forhold til deres livsstil.
6. Apo-Nett kan utveksle kunders kjøpshistorien i Apo-Nett med andre tjenestetilbydere (f.eks. treningssenter og solstudioer) som kan tilby relevante varer og tjenester ut ifra kundenes kjøpshistorikk.

Designerne ønsker å la kunder gi tilbakemelding på produkter de har kjøpt, som skal vises som del av informasjonen for hvert produkt på Apo-Nett sine åpne nettsider.

7. Kunder kan bedømme produkter de har kjøpt med 1 – 5 stjerner.
8. Kunder kan skrive kommentarer til produkter de har kjøpt, der kundens navn vises.

Apo-Nett skal ikke ha fysiske butikker. Varene leveres hjem eller hentes på postkontor eller i butikk. Designerne foreslår å sette opp grensesnitt med eksterne leverandører av varer og tjenester, som f.eks. produktleverandører, transport og logistikk.

9. Grensesnitt til eksterne leverandører er sikret med sertifikater og kryptering

Designerne foreslår en amerikansk skyleverandør, og setter følgende generelle sikkerhetskrav:

10. Skyleverandøren er ansvarlig for nettverkssikkerhet (brannmur, IDS, logg og analyse av nettverkstrafikk) og hendelsesrespons for nettverkshendelser.
11. Skyleverandøren tar ansvar for å håndtere angrep mot selve sky-plattformen, men håndterer ikke angrep mot Apo-Nett sine applikasjoner .

Gjennom sky-avtalen har Apo-Nett ansvar for spesifikke sikkerhetsaspekter:

12. Apo-Nett har ansvar for sikkerhet i web-applikasjoner, back-end server og database, men har ikke definert en spesifikk plan for hendelsesrespons eller beredskap.
13. Apo-Nett konfigurere nettverksinnstillinger etter behov, f.eks. hvilke porter som skal være åpne og lukket, og mot hva (Internett, andre grensesnitt, interne tjenester, etc.).
14. Web-grensesnittet sikres med serversertifikat og HTTPS.

Ansatte i Apo-Nett logger seg inn på PaaS-plattformen gjennom AD (Active Directory).

15. Apo-Nett foreslår å leie en AD-løsning som en SaaS (Software-as-a-Service) fra samme skyleverandør hvor de leier PaaS-plattformen.
16. Ansatte (administratorer og DevOps-utviklere) i Apo-Nett bruker et enkelt selvdefinert passord for innlogging gjennom AD til PaaS-plattformen.

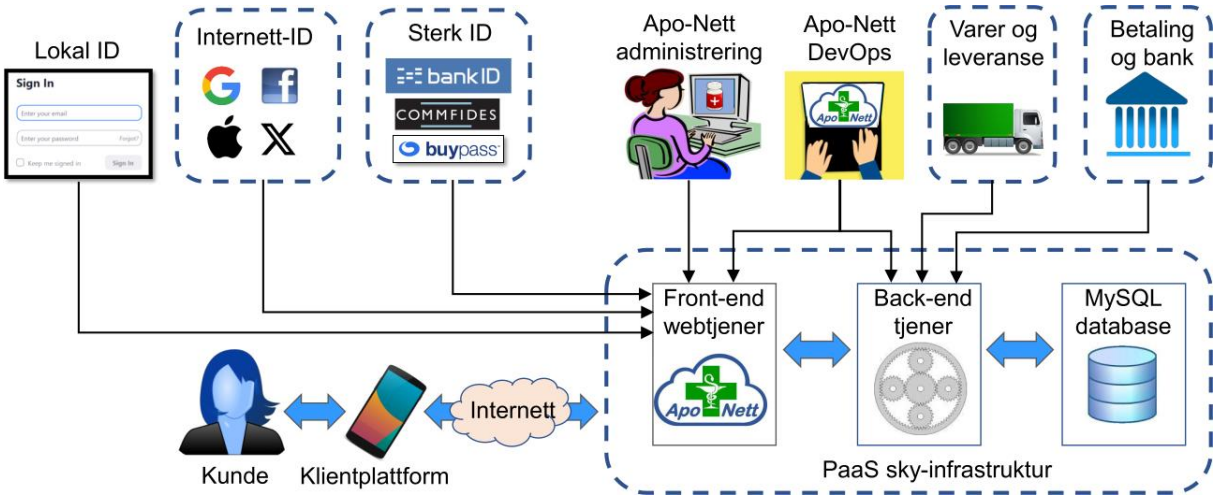
Administrering av Apo-Nett er via et web-grensesnitt for f.eks. å oppdatere produktkatalogen, vedlikeholde kunderegisteret, og samarbeid med eksterne leverandører av varer og tjenester.

17. For administrering skal Apo-Nett ha ansatte i Norge som kjenner apotek-markedet.

Utvikling og drift av Apo-Nett gjøres som DevOps, dvs. at utvikling og drift av Apo-Nett plattformen i skyen er knyttet tett sammen.

18. For utvikling og drift av web-plattformen forslår Apo-Nett å leie DevOps-utviklere i India, og det kreves ikke spesifikk kompetanse i applikasjonssikkerhet.

Overordnet arkitektur for Apo-Nett er illustrert i Figur 2 nedenfor.



Figur 2. Apo-Nett arkitektur

Oppgave C.1 (teller 20%)
Det samles inn betydelige mengder personopplysninger i den foreslåtte Apo-Nett løsningen. Etter definisjonene fra GDPR regnes Apo-Nett som «den behandlingsansvarlige», mens skyleverandøren er «databehandleren». Oppgaven består i følgende:

- Skrive en enkel DPIA-rapport som dokumentere følgende:
  a. Beskrivelse av den planlagte behandlingen av personopplysninger, som inkluderer beskrivelse av behandlingsgrunnlag. I tilfelle det planlegges overføring av personopplysninger til land utenfor EU/EØS skal også overføringsgrunnlag beskrives. For hver type personopplysning nevnt i spesifikasjonskrav (2) over, skal det beskrives hvorfor det er nødvendig å behandle denne personopplysningen, og hvorfor løsningen for Apo-Nett ikke ville fungere foruten.

  b. Vurdering av om utførelse av en DPIA er nødvendig (som leder til punkt c).

  c. Utfør DPIA som består i å beskrive relevante personvernkonsekvenser som følge av den planlagte behandlingen, der det skal vurderes om hver av disse er akseptable. DPIA er ikke det samme som å gjøre risikoanalyse, ikke bruk risikomatrise!

  d. I tilfelle noen personvernkonsekvenser av den foreslåtte behandlingen anses som uakseptable, skal det foreslås endringer i ett eller flere av spesifikasjonskravene over (1– 18) for den planlagt løsningen for Apo-Nett, slik at behandling vil være akseptabel og i samsvar med GDPR.

Oppgave C.2 (teller 10%)

Apo-Nett forvalter verdier som kan utsettes for sikkerhetstrusler. Oppgaven består i følgende:

- Beskriv et enkelt register over 3 verdier i Apo-Nett, der hver verdi er beskrevet med relevante attributter, som f.eks. hvilke typer sikkerhetsbrudd som er mest alvorlig. Gjør beskrivelsen relativt generell, det er ikke nødvendig å beskrive detaljerte verdier. Det som er viktig er ikke hvilke verdier som beskrives, men hvordan de beskrives.

Oppgave C.3 (teller 30%)

Det oppstår sikkerhetsrisikoer i den grad Apo-Nett sine verdier er sårbar for relevante trusler. Det kan f.eks. antas at trusselaktører har som målsetting å ta over kundekontoer og deres innkjøpshistorie, stjele kundedatabasen (og passord), sabotering, DDoS eller vandalisering av nettsiden, eller kjøre skadevare (f.eks. XSS, trojanere, exploits, løsepengevirus) på serverene. Dette er bare noen eksempler, det fins mange andre angrepsmålsettinger. Disse truslene skaper betydelige risikoer som må behandles slik at restrisikoen er akseptabel.

- Skriv en enkel rapport som dokumenterer risikostyring i form av risikovurdering og foreslått risikobehandling. For utførelsen av risikovurderingen skal regnearket som ligger på nettsiden for semesteroppgaven benyttes. Rapporten skal inneholde:

a. Bestem et kvalitativt nivå for akseptabel risiko.

b. En risiko består av et mulig trusselscenario som utnytter sårbarheter og skader verdier. Hvis det samme trusselscenarioet kan føre til to ulike skader på verdier, kan det regnes som to ulike risikoer. Beskriv to ulike trusselscenarioer med tilhørende risiko for hvert trusselscenario. Beskriv i tillegg en 3. risiko som forårsakes av samme trusselscenario som i en av de to foregående risikoene, men med en ulik konsekvens. Til sammen skal altså tre risikoer beskrives. Ved beskrivelse av risikoene, ikke bli stående fast pga. mangel på detaljer i case-beskrivelsen av Apo-Nett, du/dere kan gjøre passende antagelser hvis nødvendig. For hver risiko skal punktene (i-v) nedenfor beskrives.

   i. I beskrivelsen av hver risiko skal følgende elementer inkluderes. Hvis et element er irrelevant, skal dette nevnes.
      - Kort beskrivelse av risikoen (trusselscenario, hvilke sårbarheter kan utnyttes i angrepet og hvilke verdier som skades)
      - Sannsynlighetsvurdering (hvilke faktorer påvirker sannsynlighet?). Estimer sannsynlighet for hendelsen.
      - Konsekvensvurdering (hvilke konsekvenser kan hendelsen få?). Estimer helhetlig konsekvens for hendelsen.
      - Eksisterende sikkerhetstiltak (fins allerede tiltak som stopper/bremser trusselen?)
      - Deteksjon/etterforskning (fins det måter å oppdage/etterforske et slikt angrep?)

   ii. Foreta en kvalitativ risikoanalyse av risikoen som inkluderer kvalitativ estimering av sannsynlighet og konsekvens for hver risiko, og beregning av risikonivå. Hvis relevant, beskriv uvisshetsmomenter ved estimering av sannsynlighet og konsekvens for risikoen. Det fins ingen korrekt estimering av sannsynligheter og konsekvensnivå, det som er viktig er å benytte estimeringene korrekt i risikoberegningen.

iii. Gjør en kvantitativ analyse av hver risiko ved å konverter den kvalitative risikoanalysen til kvantitativ. I regnearket gjøres dette ved å bestemme det snareste en hendelse er antatt å inntreffe (som en hendelsesfrekvens *S* per år), og bestemme den verst tenkelige konsekvens (som en pengeverdi *V*).

iv. Foreslå måter å behandle risikoen i den grad risikonivået ligger over nivå for akseptabel risiko. Følgende typer behandling kan vurderes. Det skal begrunnes hvorfor en behandlingsmåte velges.
   - redusere sårbarhet gjennom å innføre sikkerhetstiltak som kan blokkere eller redusere trusselen slik at sannsynlighet for hendelse reduseres,
   - endringer i arkitektur og kravspesifikasjon for Apo-Nett, som vil bidra til å redusere risikoer, f.eks. ved å modifisere konsekvensen,
   - overføre risikoen, f.eks. gjennom å kjøpe cyberforsikring.

   Når det er relevant, skal beskrivelsen av risikobehandlingen peke på spesifikke sikkerhetstiltak som velges fra NSMs grunnprinsipper for IKT-sikkerhet:

   https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet/ta-i-bruk-grunnprinsippene/

v. Foreta ny risikoanalyse av risikoen, basert på antagelse om at foreslått behandling av risiko er blitt gjennomført. Dette gir restrisikoen.

c. Til slutt skal det lages en samlet visualisering av de tre risikoene, før og etter behandling.

Vurderingskriterier

De tre oppgavene teller 100% til sammen. For hver av de tre oppgavene legges det vekt på følgende aspekter (med relativ vekt i parentes)

- Bruk av metoder (relativ vekt 0.5)
- Struktur og fremstilling (relativ vekt 0.5)

Lever 1 pdf-fil som inneholder besvarelsen på alle tre oppgavene.

Husk å alltid oppgi referanser for figurer og andre elementer som hentes fra eksterne kilder, ellers blir det plagiering.

Oppgavebesvarelsen kan skrives på norsk eller engelsk. Typisk lengde på besvarelsen er 5000-10000 ord, som omtrent tilsvarer 10-15 sider. Å levere en lengre besvarelse er helt greit, men teller hverken positivt eller negativt.

Innleveringsfrist er mandag 11. april 2025, i Inspera.