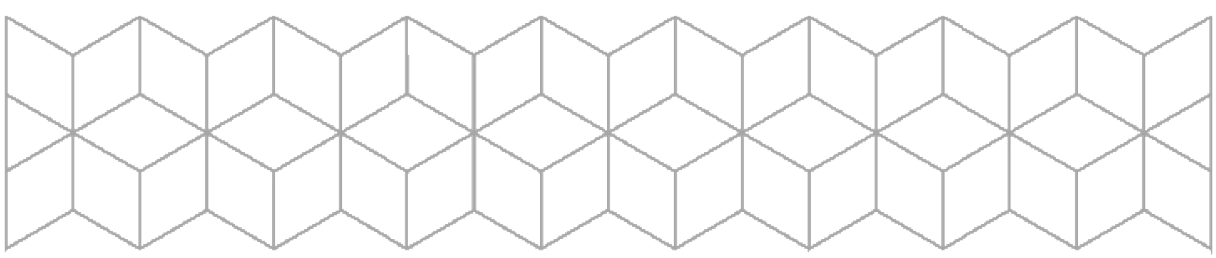
Høgskolen i Østfold

SENSORVEILEDNING

Emnekode:	ITF15019
Emnenavn:	**Innføring i datasikkerhet**
Eksamensform:	**Hjemmeeksamen – vurderes med bestått / ikke bestått**
Dato:	15/5 2020
Faglærer(e):	Tom Heine Nätt
Eventuelt:	



Eksamensoppgaven består av tre oppgaver. En kort redegjøring for hva som bør være med i oppgavene for en god besvarelse. Det er sensors oppgave å vurdere hvor grensen mellom bestått / ikke bestått skal gå, men følgende er presisert fra høgskolen:

«… vi kan ikke skjerpe kravet til studentene så nær eksamen (kreve kunnskaper tilsvarende kravene for C for å få bestått). Det vil kunne være i strid med det som opprinnelig er angitt i studieplanen, hvor studentene er blitt informert om at de trenger kunnskaper tilsvarende en E for å dekke kravet ved karakterskala A-E.

Dersom vi fraviker fra gradert skala, kan vi ikke skjerpe inn kravet til hva som må til for å bestå emner. HiØ har lagt seg på anbefalingen fra UHR, og vi konverterer ikke mellom karakterskalaene. Ved opptak til videre studier, tas ikke vurderingen "Bestått" med i poengberegningen.»

Oppgave 1:

Sikkerhetsrådene studenten gir bør være korrekte og det vekstlegges at de er rettet mot målgruppen. Rådene bør være på et nivå som gjør dem allment nyttige innenfor målgruppens bruk. Råd som rettes mot helt konkrete eksempler på angrep/svindler er ikke like aktuelle. Rekkefølgen i rådene bør følge viktighetsgraden. Studenten kan selv velge hva som menes med viktighet, men dersom ikke noe er presisert bør man anta at det betyr de rådene som reduserer risiko mest (sannsynlighet og konsekvens)

Svært viktig er studentenes begrunnelse for rådene. Dette er i hovedsak det momentet som skal hindre at studenten bedriver avskrift fra andre kilder under eksamen.

Oppgave 2

a) Her står studenten helt fritt til å velge hvilke problemer man vil se på, men som oppgaveteksten også antyder bør studenten vise at de beherskes sikkerhetsforståelse på både et teknisk og mer menneskelig plan.

Det er positivt om studenten klarer å "tenke seg litt inn i caset" og koble noen sammenhenger. Typisk slik som at ansatte legger inn informasjonen på sjefens maskin, kan bety at de har tilgang på sjefens passord eller at maskinen ikke låses. Videre at ansatte da også kan få tilgang på annen personalinformasjon de ikke skal ha.

Det er ikke satt noen krav til omfang i besvarelsen og antall problemer som skal identifiseres, men det bør reflektere prosentangivelsen i forhold til tilgjengelig tid.

b) Her forventes det at studenten gjør en ROS-analyse med å sette opp kategorier av sannsynligheter og konsekvenser, samt akseptabelt risikonivå. Videre at studenten estimerer sannsynlighet og konsekvens for de tre hendelsene og viser dette som en del av ROS-analysen. Til slutt bør studentene forklare hvordan mulige tiltak reduserer sannsynlighet, konsekvens eller begge.

Det er ingen krav til hvilken type ROS-analyse man gjør, men om det ikke er en velkjent modell bør studenten argumentere god for sin "egen løsning".

c) Her bør studenten påpeke hvordan man krever samtykke for å oppbevare informasjon, og muligens problematisere det at det samles informasjon (bekymringsmeldinger, pedagogiske observasjoner) som ikke man har direkte innsyn i. Det bør forklares at man med GDPR må ha gode rutiner for både sikkerhet og internkontroll. Mange av sikkerhetshendelsene studenten finner i a, burde være ting man på forhånd visste var et mulig problem, og som dermed GDPR krever at man rydder opp i. Det er positivt om studenten kobler svaret i c mot hendelsene i a

Mer overordnet bør det som minimum nevnes bøter/gebyrer i GDPR samt at ansvaret legges på de som samler opplysningene, ikke de som "hacker". Det bør også nevnes at bøtesatsene gjør det "lønnsomt" å satse på datasikkerhet, og som endrer holdningen. Kanskje spesielt i en barnehage med sitt noe spesielle "kundeforhold".

Oppgave 3

Det vesentlige her er at studenten klarer å velge et eksempel som illustrerer teknikken. Det burde holde med en URL og forklaringen om at dette er ekstra skadelig dersom det gjelder en "innlogget tjeneste". Samtidig bør det nevnes hvordan offeret "kjører" denne URL-en gjennom iframes, <img> eller lignende.

Eksempler nevnt i forelesning, som ikke fult ut kan klassifiseres som "eget eksempel":

- Akjsehandel
- Facebook-venneforespørsel
- Facebook-post
- Google-søkehistorikk
- Timepåmelding i treningssenter