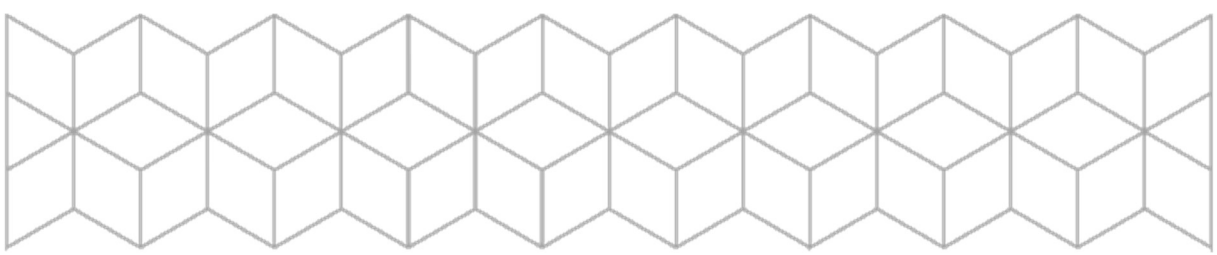
Høgskolen i Østfold

SENSORVEILEDNING

Emnekode:	ITF15019
Emnenavn:	**Innføring i datasikkerhet**
Eksamensform:	**Skoleeksamen**
Dato:	06/05-2022
Faglærer(e):	Tom Heine Nätt
Eventuelt:	



Karaktersetting

Generelt skal karakteren settes basert på et helhetsinntrykk/helhetsvurdering av besvarelsen, ikke direkte på poenggivning i oppgaver og grenseverdier på en totalscore. Del 1 og del 2 er imidlertid mulig å sensurere med en stor grad av "automatikk" og poengscore. Disse to delene teller til sammen 50 %, og skal settes sammen med helhetsvurderingen.

Del 1

Kommentar: Feil svar skal telle negativt på en slik måte at det ikke er noen hensikt å gjette. I praktisk vil det bety -1 poeng på feil svar, 1 poeng på riktig. Ingen svar gir da 0 poeng.

1. Usant
2. Sant
3. Sant
4. Usant
5. Usant
6. Usant
7. Usant
8. Usant
9. Sant
10. Sant
11. Usant
12. Usant
13. Usant
14. Usant
15. Usant
16. Sant
17. Usant
18. Sant
19. Sant
20. Usant
21. Sant
22. Usant
23. Usant
24. Sant
25. Usant
26. Usant
27. Usant
28. Sant
29. Sant
30. Usant

Del 2

Kommentar: Feil svar skal telle negativt på en slik måte at det ikke er noen hensikt å gjette. I praktisk vil det bety -1/3 poeng på feil svar, 1 poeng på riktig. Ingen svar gir da 0 poeng.

1: Tiltak som reduserer sannsynlighet for eller konsekvens av hendelsen (og i noen tilfeller også begge deler)

2: En hacker angir deler av SQL-kode som input til et system gjennom for eksempel et skjema på en nettside

3: En teknikk hackere benytter for å finne ut hvilke tjenester som kjører på en maskin

4: Vi sparer tid og prosesseringskraft ved å kun signere/verifisere hash-koden til dokumentet istedenfor selve dokumentet

5: En standardisering innen informasjonssikkerhet

6: Hackeren kan avlytte trafikken i HTTPS-kommunikasjon til legitime servere/nettsider

7: Gjøre oppbevaring av informasjon om en brukerkonto tryggere der brukere har dårlige/vanlige passord

8: White hat hacker

9: Passordet med tre tilfeldige ord er vesentlig sikrere

10: Tjenester og data som er plassert i en mer åpen sone i nettverket enn det interne nettverket

11: Sørge for at filens lagringsområde på disken overskrives av noe annet

12: Datasikkerhet er en del av informasjonssikkerhet

13: Benytte en allerede eksisterende sesjon i en tjeneste, og dermed "bli brukeren"

14: Alle bedrifter/organisasjoner med europeiske kunder/brukere

15: Dra nytte av de gode egenskapene fra hver av de (nøkkelutveksling, hurtighet osv.)

16: Ingen av de andre alternativene

17: Bedriften har blitt utsatt for et angrep eller kunne ha blitt utsatt for et angrep som går ut over brukernes personopplysninger

18: Et mål for konsekvens og sannsynlighet av en trussel

19: Personopplysningsloven er basert på/inneholder GDPR

20: Liste over gyldige tegn/input

Generelt for del 3 og 4

Det er en del av den enkelte sensors mandat å vurdere hvordan uttelling skal gis på svarene i de ulike oppgavene, og hva som er et akseptabelt nivå. Dette vil også være en del av diskusjonen mellom sensorene ved sensureringen.

Resten av denne sensorveiledningen gir noen stikkord til momenter som bør være med i et godt svar (enkeltmomenter kan erstattes av andre, da det ikke nødvendigvis er forventet at studentene kommer på nettopp disse). **Merk at sensorveiledningen ikke er en komplett liste med alle momenter eller nødvendigvis reflekterer noe A/B-svar**. Studentbesvarelser bør utdype momentene mer, og sette de i en sammenheng, slik at sensor kan være trygg på at teorien er forstått og ikke bare pugget/tilfeldig.

Hovedhensikten med denne sensorveiledningen er å gi sensor et innblikk i relevant pensum som kan passe i de ulike oppgavene. Det er altså ikke et løsningsforslag.

Sensorene må også se på hvordan kandidatene som en gruppe har løst eksamenssettet og legge forventingene på hver oppgave deretter. I og med at det er nærmere 200 besvarelser i emnet vi en slik vurdering være mulig å gjøre korrekt.

Del 3

3.1

A + B) Noe man er (fingeravtrykk, retina), noe man har (SMS, kodebrikke) og noe man vet (passord, PIN). Gode studenter bør også diskutere inn "lokasjon" som en egen faktor eller deler av andre faktorer

Kommentar: Innholdet i oppgave A og B bør være godt kjent for studentene, og er en forholdsvis lett memorerbar faktaopplysning. Det forventes derfor at også middels studenter har forholdsvis komplette svar på denne, samt at mangler trekker vesentlig ned.

c) Krever mer kunnskap hos brukere og mer support hos tjenestene. Kan være forbundet med en kostnad (utsending av SMS, utvikling, drift etc.) Obligatorisk to-faktor-autentisering ville gjort registreringsprosesser mer komplisert (og flere kunne falt av).

3.2

a) Kun samle og lagre persondata som er nødvendig for å oppfylle formålet

b) Innsamlet data kan kun benyttes til det/de formålet/-ene som er opplyst brukeren. For å benytte persondata til noe utenfor formålet må det innhentes nytt samtykke

c) Opplysninger fjernes (evt. anonymiseres) så snart man vet at det ikke lenger er behov for dem.

d) Handlingen som gjøres og loggføres når en bruker aksepterer innholdet i personvernseklæringen

e) Informasjon om hvilke data som samles inn, hva de skal benyttes til. Er en del av det man samtykker til.

Kommentar: Det er viktig at de gode studentene klarer å skille samtykke og personvernserklæring fra hverandre i sine forklaringer, selv om det i utgangspunktet kan se ut for å være en overlapp.

3.3

a) Kandidaten bør forklare hvordan man i det skjulte blir lurt (gjennom linker/nettsider) til å utføre handlinger i tjenester som ellers iverksettes av knapper, skjemaer osv i tjenesten. Handlingene knyttes til brukeren dersom brukeren er logget inn i tjenesten. Gode studenter bør også trekke frem at handlinger kan knyttes til brukeren også uten innlogging, ved at elementer plasseres i nettleserens historikk, detekteres i nettrafikk, cookies osv.

Kommentar: Det kreves ingen dyptgående forklaring av detaljer i webteknologien, men prinsippene i teknologien/fremgangsmåten må forklares såpass at det definerer denne angrepsformen, og svar som "noen får deg til å gjøre handlinger" blir for generelle.

Her bør det gis et eksempel dersom kandidaten ikke klarer å forklare detaljert nok med tekst. Gjerne med GET da det krever mindre forklaring. Typisk noe ala dette:

Bruker får en e-post med følgende lenke: https://www.nettbutikk.no/kansellerOrdre?ordreid=21234

Når bruker trykker på linken, og er innlogget i tjenesten, utføres samme handling som om brukeren selv hadde trykket på en link "kanseller ordre" i selve tjenesten.

b) Brukeren er helt avhengig av tiltak som gjøres av tjenesten selv for å teknisk stoppe CSRF. De færreste er i stand til å se om gode tiltak er på plass eller ikke. Brukens muligheter er upraktiske, slik som å alltid logge ut av en tjeneste/benytte ulike nettlesere/sjekke linker. I praksis er det derfor umulig for brukerne å sikre seg.

Kommentar: Selv om ikke oppgaven spør etter det, så vil nok enkelte studenter kun ramse opp mulige mottiltak for brukeren mot CSRF. Dette kan gi en liten uttelling, men et godt svar bør diskutere prinsippet beskrevet over. Prinsippet er nevnt, men ikke mye omhandlet i pensum/forelesning. Denne oppgaven er med for å teste studentenes egen refleksjon over pensum.

3.4

a) Falskt advarsel om en sikkerhetstrussel/problem i form av informasjon på nettsider, oppringning, e-post, annonser, programvare (skadevare) eller lignende som ønsker å skape frykt, status og/eller få brukeren til å utføre handlinger. Bygger på prinsipper fra sosial manipulasjon.

b) Her bør kandidaten nevne ulike eksempler (ulike fremgangsmåter/prinsipper). Varianter av samme eksempel (kun tema el.l. som er endret) bør ikke gi uttelling for gjentakelsen(e) av varianten. Typisk på formen (ett av mange mulige eksempler); Mottar en e-post som forteller at du muligens har en skadevare, og en fremgangsmåte for å sjekke om man har det (for eksempel oppslag i Windows registeret). Når bruker ser at informasjonen stemmer med sin maskin, laster brukeren ned et verktøy for å fikse problemet som e-posten henviser til, men verktøyet er i seg selv skadevare. Brukeren er altså blitt lurt til å selv installere en skadevare gjennom falsk informasjon om et sikkerhetsproblem brukeren ikke hadde.

c) Ingen absolutt liste, men bør kunne nevne ting som: gjøre googlesøk på informasjon, ikke ta i mot hjelp av de som forteller om et problem, få andre til å se på advarselen, være kritisk til meldinger som skaper frykt/problem-følelsen osv.

Kommentar: En god besvarelse vil også kunne trekke inn mer konkrete mottiltak mot konsekvensene som 2FA og antivirusverktøy samt mer tekniske sikkerhetsmekanismer som spam-filtere osv. Men å kun liste opp konkrete mottiltak mot konsekvenser/tekniske sikkerhetsmekanismer og ikke noen mer generelle metoder for å avsløre hoax er ikke en fullgod besvarelse.

3.5

Her er det vesentlig at kandidaten får frem at det er en kryptert kanal mot et fast endepunkt (ikke mot mottaker) som har til hensikt å beskytte kommunikasjon på ukjente nettverk mot avlytning og modifikasjon.

En god besvarelse bør også ha med poenget om at selv om HTTPS og lignende kryptering uansett gjør det vanskelig å avlytte, vil man ikke være sikret mot trafikkanalyse (hvem, når) samt endring av nettverksinforasjon, slik som DNS-server.

Typiske bruksområder er når man er på et nettverk man ikke stoler på, eller ønsker tilgang på interne ressurser i et nettverk, men sitter eksternt.

Kommentar: Det vil telle negativt om kandidaten for eksempel sier at VPN sikrer anonymitet ovenfor en tjeneste eller at det er kryptert helt til mottaker (så sant det ikke er VPN-endepunktet)

Del 4

Denne delen har ingen gitt fasitsvar. Det er likevel noen momenter som man burde kunne forvente at er med (meget kort skissert under). Merk at dette kun er noen få momenter, og ikke en liste over hva som er et godt nok svar.

Det forventes at studenten evner å vise både dybde- og breddekunnskap, samt reflekterer over hele datasikkerhetsområdet fra det tekniske til det organisatoriske/personlige.

Et vesentlig moment i oppgaven er begrepet "drøft". Kandidaten skal altså i en stor grad komme med egne synspunkter/tanker og diskusjon, ikke ramse opp pugget fakta om temaene. Kandidaten skal altså vise evne til refleksjon over pensum som er lært, og det er denne evnen som skal vektlegges i vurderingen av svaret.

1)

- Vanskelig å oppdage/avverge trusler fordi det krever opplæring/kunnskap ikke et verktøy (privat/bedrift)
- Opplæring er vanskelig
- Tekniske tiltak og sikkerhetsmekanismer kan sjelden hindre brukere å utføre ting de har bestemt seg for (etter påvirkning)
- Lite tjenester kan gjøre for denne typen sikkerhetstrusler

- Når målet for angriperne ikke lenger er å "vise teknisk kompetanse" blir enkleste vei brukt (som ofte er sosial manipulasjon)

2)

- Krav om sikkerhetsarbeid (internkontroll etc)
    - kan også dra med seg andre områder enn direkte mot personopplysninger
    - komplett gjennomgang
    - bevisstgjøring i alle organisasjonsnivåer
- Påvirker både konsekvenser (bøter, plikt til å varsle/dårlig PR etc) og sannsynlighet for tap (bøter uten at hendelser har skjedd, plikt til å varsle etc) som gjør det mer lønnsomt å satse på datasikkerhet
- Alle stiller likt. Ingen taper på å være den eneste som skjerper sikkerheten.
- Bransjestandarder og organisasjoner jobber felles med sikkerhet (alle må gjøre noe)