Veiledning til fasit for eksamen IN1020
Seksjon 3 «Datasikkerhet» H25

Oppgave 3.1 Sikkerhetsmål

0,33 poeng for hvert riktige svar, ingen minuspoeng.

I denne oppgaven må man kunne de helt grunnleggende egenskapene ved ulike sikkerhetsmål. Se korrekte svaralternativer i fasiten, samt forelesning og øvingsoppgaver for detaljerte definisjoner av disse seks sikkerhetsmålene det er spurt om i oppgaven.

Oppgave 3.2 Brudd på sikkerhetsmål

0.5 poeng for hvert riktige svar, ingen minuspoeng.

- Endring av nettverkstrafikk: Brudd på **integritet** som følge av mulig uautorisert endring/sletting av datapakker.
- Løsepengevirus: Brudd på **tilgjengelighet** - et løsepengevirus krypterer data/filer slik at de blir uleselige/utilgjengelige for de som skal ha rettmessig tilgang.
- Tjenestenektangrep: Brudd på **tilgjengelighet** - en tjeneste angripes på en slik måte at den ikke responderer på normale (rettmessige) forespørsler og er dermed utilgjengelig.
- Spionprogramvare: Brudd på **konfidensialitet** - spionprogramvare har til hensikt å spionere på (bruken av) datamskiner eller IT-tjenester med mål om å få tilgang til informasjon.
- Falsk digital ID: Brudd på **autentisitet** - den som benytter en falsk ID utgir seg for å være en annen.
- Avlytting nettverkstrafikk: Brudd på **konfidensialitet** siden uautorisert avlytting av nettverkstrafikk kan føre til at data/informasjon kommer på avveie.

Oppgave 3.3 Begrepsforståelse - Kombiner riktig begrep med riktig tekst

0.5 poeng for hvert riktige svar, ingen minuspoeng.

De korrekte alternativene er tydelige i fasiten. For utsagnet ".... kan brukes til å få tak i data direkte fra en database." gir i tillegg svaret *Sårbarhet* 0.25 poeng, mens *SQL-injeksjon* er teknikken som ofte brukes for uautorisert tilgang til databaser via spørrespåket SQL, og som her er det mest presise svaret som gir full pott med 0.5 poeng.

Forklaring på begrepene som ikke er korrekte og som dermed er til overs:

- *Sårbarhet* er en feil eller en svakhet i et dataprogram som åpner for mulighet til å utnytte systemet.
- *Dataminimering* er prinsippet om at det aldri skal behandles (heller ikke lagres) flere personopplysninger enn det som er nødvendig.
- *Cross site scripting* er injisering av ondsinnet kode i tilsynelatende pålitelige nettsteder.
- *Symmetrisk nøkkel* er den hemmelige nøkkelen brukt til kryptering/dekryptering i symmetrisk kryptering.
- *Autorisering* er det å spesifisere tilgangsrettigheter.
- *Digitale sertifikater* har til hensikt å hindre falske offentlige nøkler, og knytter sammen en identitet med en tilhørende offentlig nøkkel).

Oppgave 3.4 Tilgangskontroll

0.5 poeng for hvert riktige svar, ingen minuspoeng.

(a) Autentisering i kombinasjon med autorisasjon er korrekt svar. For å kunne utføre tilgangskontroll må det først foreligge kunnskap om *hvem* som ber om tilgang. Deretter må en forespørsel sjekkes mot forhåndsdefinerte tilgangsrettigheter, og det å spesifisere slike tilgangsrettigheter kalles *autorisasjon*.

(b) Riktig definisjon av tilgangskontroll er dermed alternativet "Tilgangskontroll er å håndheve definerte tilgangsrettigheter i et datasystem."

(c) Tilgangskontroll er et *forebyggende* sikkerhetstiltak, det er et tiltak som iverksettes for å *unngå* at uautoriserte får tilgang til informasjon eller ressurser de ikke skal ha tilgang til.

(d) Feil i et system som håndterer tilgangskontroll kan faktisk føre til brudd på både konfidensialitet (noen får uautorisert tilgang til å lese informasjon), integritet (noen får uautorisert tilgang til å endre/slette informasjon), og tilgjengelighet (autoriserte som skulle hatt tilgang hindres i å få tilgang).

Oppgave 3.5 Anvendelse av kryptografi 1

0.5 poeng for hvert riktige svar, -0.3 for hvert gale svar

(a) Alice og Bob bruker i denne deloppgaven symmetrisk kryptering (felles hemmelig nøkkel), og utgangspunktet er at både Alice og Bob - men ingen andre - kjenner denne nøkkelen. Når Alice sender en kryptert melding til Bob som han kan dekryptere med den sammen hemmelige nøkkelen kan han dermed være sikker på at meldingen kommer fra Alice (med mindre han ha sendt den selv). Alice kan også være sikker på at meldingen kun kan leses av Bob, som er den eneste andre som kjenner nøkkelen. En tredjepart (her Eve) kan derimot ikke være sikkert, siden hun ikke kan vite om det er Alice eller Bob som har kryptert meldingen, begge to har jo tilgang til den hemmelige nøkkelen.

Denne måten å sende melding på sikrer konfidensialitet, siden ingen andre enn Alice og Bob kjenner krypteringsnøkkelen og kan dekryptere og lese en melding kryptert med denne nøkkelen.

(b) I denne deloppgaven bruker de asymmetrisk kryptering, med et nøkkelpar der Alice har den private (hemmelige) nøkkelen, mens Bob og alle andre får tilgang til den tilhørende offentlige nøkkelen. Når Bob får en melding fra Alice som han kan dekryptere med Alices offentlige nøkkel

kan han være sikker på at den er kryptert med Alice sin private nøkkeol, og at meldingen dermed kommer fra henne. Alice kan derimot ikke være sikker på at meldingen leses av bare Bob, den kan dekrypteres og leses av alle med tilgang til den offentlige nøkkelen. En tredjepart (f.eks. Eve) kan også være sikker på at meldingen kommer fra Alice, siden det her kun er Alice som kjenner den private nøkkelen og kan bruke den til å kryptere en melding.

Denne måten å sende melding på sikrer **ikke** konfidensialitet, siden alle med tilgang til den offentlige nøkkelen kan dekryptere og dermed lese meldingen.

Oppgave 3.6 Anvendelse av kryptografi 2

0.5 poeng for hvert riktige svar, ingen minuspoeng

(a) Korrekt svar kommer tydelig fram i fasiten. For digital signering med asymmetrisk kryptering bruker den som signerer sin private nøkkel (som ingen andre kjenner), mens den som skal verifisere signaturen må bruke den tilhørende offentlige nøkkelen. Dette sikrer *uavviselighet*.

(b) Korrekt svar kommer tydelig fram i fasiten: For å sende konfidensielle meldinger med asymmetrisk kryptering må avsender bruke mottagers offentlige nøkkel for å kryptere, mens mottager bruker sin tilhørende private nøkkel (som ingen andre kjenner) for å dekryptere og lese meldingen. Dette sikrer *konfidensialitet*.

Oppgave 3.7 Personopplysningsvern

(a) 1 poeng for riktig svar, ingen minuspoeng

Arbeidsgiver er minimum pliktig å vurdere om de har *hjemmel* til å behandle de nevnte personopplysningene om sine ansatte, og spesielt vurdere nødvendighet mtp. at noen av opplysningene er i kategorien *særlige kategorier av personopplysninger*.

(b) 0.5 poeng for hvert riktige svar, -0.3 for hvert gale svar

Riktig svar er *Religiøs overbevisning*, *Politisk oppfatning* og *Etnisk opprinnelse*. Merk at *fødselsnummer* ikke er i kategorien særlig kategori av personopplysninger, men skal i følge lovverk likevel kun brukes/behandles når det er helt nødvendig.

(c) 0.5 poeng for hvert riktige svar, -0.3 for hvert gale svar

Riktig svar er "Krav til at personopplysninger som hovedregel ikke benyttes til andre formål enn det de er samlet inn for" (prinsippet om formålsbegrensning), "Krav om at det ikke registreres flere personopplysningen enn nødvendig for behandlingen" (prinsippet om dataminimering), samt "Krav om at informasjonssikkerhet ivaretas i behandlingen".

Svaralternativet "Krav om at opplysninger arkiveres i fall det dukker opp nye behandlingsbehov" strider mot prinsippene om formålsbegrensning og lagringsbegrensning. Det er også slik at selv om den registrerte har samtykket til en behandling av personopplysninger om seg, er det en rekke andre krav som databehandleren må oppfylle (f.eks. krav til å ivareta informasjonssikkerhet).

Oppgave 3.8 Trusselmodellering og risiko

(a) 0.33 poeng for hvert riktige svar, -0.2 for hvert gale svar

Trussel mot konfidensialitet:

Passordlekkasje kan føre til at uvedkommende får logget inn i systemer og får tilgang til informasjon de ikke skal ha tilgang til.

Sårbarhet i programvare via leverandørkjede kan føre til at det introduseres veier inn i systemet som omgår autentisering og tilgangskontroll, og uvedkommende kan få tilgang til informasjon de ikke skal ha tilgang til.

Phishingangrep mot ansatte kan føre til at de enten lures til å gi fra seg konfidensiell informasjon, evt. brukernvn/passord som gjør at uvendkommende får tilgang til systemer og informasjon de ikke skal ha tilgang til.

Tjenestenektangrep og løsepengevirus er ikke trussel mot konfidensialitet men mot tilgjengelighet.

(b) 0.33 poeng for hvert riktige svar, -0.2 for hvert gale svar

Å gjennomføre regelmessige sikkerhetsøvelser som bevisstgjør ansatte samt avdekker evt. sårbarheter er et godt sikkerhetstiltak for å ivareta konfidensialitet.

Å innføre tofaktorautentisering for innlogging vil kunne redusere risikoen for å bli utnyttet ved f.eks passordlekkasjer eller phishingangrep.

Å kryptere alle data som lagres kan bidra til å gjøre data uleselige selv om de kommer på avveie.

Å bruke sjekksumalgoritmer for alle data som lagres vil kunne bidra til å sikre integritet, mens det å sørge for at alle ansatte har tilgang til alle bedriftshemmeligheter heller kan betraktes som et brudd på konfidensialitet.

(c) 0.5 poeng for hvert riktige svar, -0.3 for hvert gale svar

Angrep med løsepengevirus kan føre til at informasjon krypteres av uvedkommende på en måte som gjør at de ikke lar seg dekryptere av de som skal ha tilgang, og fører dermed til brudd på tilgjengelighet.

Tjenestenektangrep har også til hensikt å overbelaste systemer/tjenester i så stor grad at de blir utilgjengelig for de som skal ha tilgang, og er dermed brudd på tilgjengelighet.

Avlytting av nettverkstrafikk både mellom kunde og bedrift samt internt i bedriften kan typisk føre til brudd på konfidensialitet, det samme gjelder spionprogramvare på en ansatts datamaskin.

(d) 0.5 poeng for hvert riktige svar, -0.3 for hvert gale svar

Det å ha gode rutiner for sikkerhetskopiering av data gjør at man raskt kan tilgjengeliggjøre ødelagte data som følge av f.eks. angrep med løsepengevirus.

Å gjennomføre regelmessige sikkerhetsøvelser som bevisstgjør ansatte samt avdekker evt. sårbarheter er et godt sikkerhetstiltak også for å ivareta tilgjengelighet. F.eks. er det lurt å øve på å hente tilbake data fra sikkerhetskopier, slik at man vet at rutiner fungerer i tilfelle angrep med løsepengevirus.

Å innføre tofaktorautentisering vil ikke påvirke tilgjengelighet til informasjon, og det vil heller ikke det å bruke sjekksumalgoritmer på lagrede data, eller å kryptere data som lagres.