Datasikkerhet fasit

Time 1:

Oppgave 1: Hvordan kan kryptografi brukes av trusselaktører til å svekke disse sikkerhetsmålene:

a) Tilgjengelighet Ved å for eksempel bruke et løsepengevirus kan en angriper gjøre slik at alle dataene dine blir kryptert. For å dekryptere dataene dine blir du bedt om å betale løsepenger.
b) Uavviselighet (Hint: hash-algoritmer) Hvis en hacker begår et kollisjonsangrep kan dette for eksempel brukes til å forfalske digitale signaturer. Jeg kan lage to dokumenter med samme hash-verdi og sende det ene til deg. Du signerer hashen og sender tilbake til meg. Jeg kan nå feste signaturen din på det andre dokumentet, med identisk hash. Du har jo i praksis bare signert hashen, så nå ser det ut som du har signert et dokument som du ikke en gang visste om!

Oppgave 2: Hvorfor garanteres ikke uavviselighet når man bruker symmetrisk eller asymmetrisk kryptering?

I symmetrisk kryptering brukes en hemmelig nøkkel til å kryptere og dekryptere dataene. Dette betyr at alle med nøkkel kunne ha sendt dataene. Altså ikke uavviselig.

I asymmetrisk kryptering er ofte nøkkelen som brukes til å kryptere dataene offentlig. Så her kan alle som har tilgang til offentlig nøkkel i teorien være avsender. Ikke uavviselig.

Oppgave 3: Hvilke sikkerhetsmål blir ivaretatt med digital signatur?

- ❑ Konfidensialitet
- ✓ Integritet
- ✓ Uavviselighet
- ✓ Autentisitet

Oppgave 4: Hva er PKI? Kan du komme på et eksempel på bruk av PKI i Norge?

PKI er et rammeverk for hvordan offentlige nøkler skal distribueres, administreres og brukes. PKI sikrer også ektheten til offentlige nøkler, siden disse er offentlige og derfor kan være utsatte. I Norge brukes PKI bl.a. i bank-id sine tjenester.

Time 2:

Oppgave 1: Du lager et IT-system som bl.a. skal håndtere personopplysninger fra brukerne dine. Du har kommet frem til at det vil være billigere og enklere for deg å kjøpe lagring hos en skytjeneste i utlandet (i EU). Hva betyr dette i disse tilfellene?

a) Når du skal inngå en avtale med en skytjeneste? Her må dere inngå en databehandler avtale, ellers er det ulovlig for deg å kjøpe skytjenester av denne databehandleren. Både

behandlingsansvarlig og databehandler har som plikt å følge reglementet i GDPR, men det er du som må forsikre deg om at databehandler følger reglementet. Dette gjelder uansett om databehandler er en liten eller stor leverandør.

b) Hvis skytjenesten lekker kundeopplysninger? Det er du som er behandlingsansvarlig, så det er til syvende og sist du som er ansvarlig selv om dataene var lagret hos en databehandler her. Så da er det vel om å gjøre at du har overholdt alle reglene om behandling av personopplysninger hvis du vil unngå straff. (Det er mer som kan sies her. For eksempel om varslingsplikt og alvorlighetsgrad. Jeg baserer svaret på hva dere gikk gjennom på forelesning.)

c) Når samarbeidet er over? Da må du forsikre deg om at opplysningene blir slettet. Det er også mulig du fremdeles trenger opplysningene, og da vil du nok ha dem overført til din server eller en annen databehandler.

Oppgave 2: Økonomisk vinning er en klar motivasjon og drivkraft i utvikling, drift og salg av IT-systemer. Hvordan kan dette være til fordel eller ulempe for brukere (kunder) av systemene?

Hvis leverandører er ute etter en kjapp penge vil de kanskje ikke prioritere sikkerhet i produktene sine. Mange billige tech-produkter som selges kommer ikke med sikkerhetsoppdateringer og er laget slik at de lett kan hackes og utnyttes. Når sikkerhetsbrudd skjer vil mange leverandører dysse ned skaden i stedet for å advare brukerne sine, siden dette fører til dårlig reklame og potensielt klager, ønsker om refundering eller rettsaker. Ofte blir informasjonssikkerhet veiet opp mot økonomisk vinning, slik at litt risiko ikke blir sett på som særlig alvorlig hvis straffen leverandøren risikerer ikke er høy. Samtidig har forbrukere kjøpekraft som betyr at leverandører som har bevist at de ikke er til å regne med kan få dårlig omdømme slik at kunder bytter tjenester. Man kan kanskje også argumentere for at ikke alle produkter blir brukt i sensitive settinger. Så å ha mulighet til å betale mindre for en mindre sikker tjeneste kan kanskje være nyttig av og til? Å ha et sikkerhetskamera i hønsehuset er for eksempel ikke like alvorlig som å ha et i stua, med tanke på om det blir hacket, men dette er kanskje litt vel optimistisk, eller?

Oppgave 3: Jeg har laget et IT-system og vil gjøre trusselmodellering av systemet. Jeg har bestemt å ha fokus på trusselaktører. Hva betyr dette?

- ❑ Jeg går gjennom hele systemet for å finne alle svakheter trusselaktører kan utnytte.
- ❑ Jeg benytter en PKI, som gjør at kun rettmessige brukere kan benytte systemet mitt.
- ✓ Jeg spør meg selv hvilke trusselaktører som kan true systemet mitt.
- ✓ Jeg tenker på hvilke verdier trusselaktører kan være ute etter.
- ❑ Jeg innfører sikkerhetsprotokoller som gjør det vanskelig for trusselaktører å bryte seg inn.
- ✓ Jeg spør meg selv hva som vil skje hvis trusselaktører klarer å hacke systemet mitt.

Risikoanalyse kommer gjerne etter trusselmodellering, men jeg har satt det siste alternativet som riktig, siden noen kilder har inkludert dette I trusselmodellering.