IN1020: Løsningsforslag gruppetime 6 (uke 40)

1. Oppgave 1, 2 og 3 er diskutert i Lærebokas bloggartikkel https://www.datasikkerhetsboka.no/blogg/2018/03/23/hva-vet-tjenestene-om-deg-og-hva-betyr-dette-for-din-sikkerhet-og-ditt-personvern/), se den for diskusjon og løsningsforslag.

2. Se over

3. Se over

4. "Internet of Things (IoT)":

   Diskuter. Alt som er på nett. TV? robotstøvsuger, trenings-/aktivitetsklokke, kjøleskap, komfyr, vaskemaskin? Lås?

5. Samfunnskritisk infrastruktur:

   Kraftverk, vannforsyning, styringssystem tog, luftfartsovervåkning, strømforsyning i -25 midt i januar? Kan potensielt bety katastrofe for mange.

6. Sikkerhetsmål: Sikkerhetsmål er altså egenskaper ved informasjonssikkerhet, egenskaper vi ønsker å oppnå eller tilby, og som på sett og vis beskriver informasjonssikkerhet. De *opprinnelige* sikkerhetsmålene er konfidensialitet, integritet og tilgjengelighet, og det er disse (også kalt *KIT eller CIT*) som er bransjestandard for informasjonssikkerhet. I tillegg kommer autentisitet, uavviselighet, sporbarhet. I dag nevnes også personvern som et sikkerhetsmål i de tilfeller det behandles personopplysninger.

   (a) Konfidensialitet betyr at informasjon ikke tilgjengeliggjøres for annet enn de entiteter, systemer og/eller prosesser som er autorisert for tilgang til informasjonen. Det kan gjelde forretningshemmeligheter, personopplysninger, eller å f.eks. sikre anonymitet der dette er nødvendig. Konfidensialitet omfatter alle typer informasjon/data, alt fra "vanlig"informasjon til f.eks. data som konfigurerer systemer og da data som er med på å styre datamaskiner.

   (b) Integritet handler om å kunne stole på at informasjon eller systemer ikke er endret eller slettet av entiteter, systemer eller prosesser som ikke er autorisert for handlingen. Brudd på integritet kan skyldes både angrep utenfra og feil i systemer som fører til korrupte data. I likhet med konfidensialitet omfatter integritet også alle typer informasjon/data.

   (c) Tilgjengelighet dreier seg om at informasjon til enhver tid skal være tilgjengelig for den som skal ha tilgang til informasjonen. Mobilnett, nødnett, pasientsystemer, banksystemer, betalingssystemer er viktige systemer vi i dag er forholdsvis avhengige av i hverdagen, og som dermed bør ha sterkt fokus på tilgjengelighet. Samtidig vil det for en nettbutikk føre til svikt i omsetningen hvis deres nettbutikk gjøres utilgjengelig for en periode, selv om det kanskje ikke berører oss forbrukere på samme måte (vi er ikke så veldig lojale, og velger raskt en annen butikk...).

   DDOS-angrep eller andre angrep som tar ned et system/en tjeneste er en trussel, men det samme er f.eks. systemfeil, feilkonfigurasjon (en ansatt har ikke fått riktige tilganger pga. manuell feilregistrering), naturkatastrofer eller strømbrudd.

   (d) Autentisitet er betegnelsen på egenskapen som forteller noe om *ektehet*, altså å vite og være viss på at alle parter er de/den som de utgir seg for å være. De fleste kan se for seg nødvendigheten av å kunne stole på at en *bruker* i et datasystem er *autentisk*, og vet hva det

er, men autentisitet er mer enn det. F.eks. at nettsiden du besøker faktisk er den nettsiden du mente å besøke, og ikke en identisk kopi noen har opprettet for å lure deg. Hovedtrusselen er at noe eller noen klarer å utgi seg for å være noen/noe de ikke er. Passord er f.eks. enkelt å stjele/gjette/knekke, og falske nettsider ganske enkelt å lage. Mer om autentisitet og ulike former for autentisering i forelesning 28. august.

(e) Uavviselighet. Det skal ikke være mulig å påstå at man ikke har gjort noe man har gjort, og at man har gjort noe man ikke har gjort. Dette gjelder f.eks om man har undertegnet en kontrakt (f.eks for boliglån), eller glemmer å overføre penger i nettbanken.

Uavviselighet er altså å bekrefte at en handling eller et informasjonselement er uendret (integritet) og at det kan knyttes til en bestemt identitet. Uavviselighet er i mange sammenhenger også omtalt om ikke-benekting. En løsning for uavviselighet er en løsning som gjør det mulig for også en tredjepart å innhente tilstrekkelig dokumentasjon for at en annen part ikke kan nekte for å ha gjennomført en handlig eller ha valgt å bekrefte/vedgå seg et informasjonselement.

En løsning for uavviselighet er bygget opp på samme måte som løsninger som sikrer autentisitet. Forskjellen er at brukeren skal være i stand til ikke bare å bekrefte hvem man er over nettet, men også å legge igjen dokumentasjon som entydig knytter personen til en handling eller et uendret informasjonselement.

(f) Sporbarhet, også omtalt som etterprøvbarhet, er egenskapen som sikrer at alle handlinger kan spores tilbake til en entydig entitet. Sporbarhet garanterer at alle operasjoner som utføres av individer (brukere, personer, systemer eller prosesser som kjøres kan identifiseres, og at sporene bevares (logges) for senere bruk.

Ved et datainnbrudd øker dette muligheten for å spore en kriminell handling tilbake til den eller de som utfører handlingen. Men fortsatt er det dessverre slik at det på tvers av landegrenser, uten felles lovverk, kan være svært vanskelig å stille gjerningsmenn til ansvar for kriminelle handlinger.

Å sørge for sporbarhet i et system vil i mange tilfeller også være med på å rette opp feil som skjer. Et eksempel er, som nevnt på forelesning, hvis du plutselig oppdager at karakteren din plutselig er endret fra en ståkarakter til stryk, uten grunn. I et system som sikrer sporbarhet vil denne endringen kunne spores, og handlingen knyttes til f.eks. en identifiserbar bruker. Personen vil kunne stilles til ansvar for handlingen, og man kan finne ut om det er en feil, sabotasje, el.

(g) Personvern stiller bl.a. krav til bl.a. *hjemmel* av behandling/oppbevaring av personopplysninger, samt skal sørge for at den registrertes rettigheter oppfylles. Personvern dreier seg også om å hindre uautorisert innsamling av data, at data som er samlet inn ikke benyttes til andre formål enn det den registrerte har samtykket til, det skal ikke lagres lenger enn nødvendig, samt at det gir den registrerte rett til innsyn i egne opplysninger, *rett til å bli glemt*, osv.

Tilleggsspørsmål: Hvis loggene som skrives og bevares for å sikre sporbarhet inneholder personopplysninger (altså opplysninger som kan knytte dem til en identifiserbar person), er dette faktisk også *behandling* av personopplysninger og omfattes av presonopplysningsloven. Her er det mange som feiler. Man er flinke til å innføre og håndheve rutiner for å slette data, mens en glemmer å rydde logger, som dermed blir lagret (for) lenge.

7. Case-oppgave:

(a) Persondata. Mange selskaper er interessert i å få tak i e-mail telefonnummer og ordrehistorikken til folk. Kundeklubb-poengene er også en verdi, siden disse kan byttes inn i rabatter.

(b) Folk som vil selge kundeinfo videre, kunder som vil jukse til seg flere poeng.

(c) Konfidensialitet bør prioriteres for å følge GDPR. Integritet er viktig for at kunders info alltid er korrekt. Uavviselighet kan være bra, slik at kunder ikke kan nekte for å ha brukt poeng eller annet.

(d) Tingangskontroll via innlogging, Integritet og uavviselighet kan opprettholdes via loggføring. Hash-algoritmer også for integritet (men dette har de ikke lært om ennå).

8. Case-oppgave:

   (a) Alt av info om spillet er en verdi. Fans vil være veldig interessert i å se konsept-tegninger, level-design, spoilere, animasjoner... etc... etc. I noen tilfeller kan det være en verdi å vite hvem som jobber med spillet, men dette er ikke så ofte hemmelig. Konkurrenter vil også være interessert i å se hvordan ting gjøres.

   (b) Fans av spillet vil ønske å få tak i alt de kan. Folk som hater spillet kan forsøke å sabotere. Ansatte kan lekke info. Konkurrenter kan ønske å stjele deler av arbeidet.

   (c) Integritet. Det verste som kan skje er nok at arbeid mistes. Konfidensialitet er også bra, slik at selskapet kan kontrollere markedsføringen selv.

   (d) Separat backup av all data. Tilgangskontroll og loggføring, slik at man kan kontrollere hvem som har tilgang til hva og hvem som har gjort hva.

9. Personopplysninger og personvern:

   (a) Ingen fasit, men en god forståelse for hva som er personopplysninger er målet. F.eks. vil en innlevering du har levert i et fag være en personopplysning selv om den ikke direkte inneholder persondata, så lenge den kan knyttes til deg som person. Enkelte *persopplysninger av særskilt karakter* er kanskje uforståelig for oss i Norge i dag, f.eks. medlemskap i fagforening, men husk at lovgivningen gjelder hele Europa, og at denne typen informasjon kan være langt mer sensitiv der. Se også på formuleringen som dreier seg om fødselsnummer.

   (b) Personopplysningsloven stiller krav om bl.a forebygging av uautorisert innsamling og lagring av personlige opplysninger, samt at innsamlede data om den registrerte ikke benyttes til andre formål enn det man har hjemmel til eller den registrerte har samtykket til. I tillegg sier lovverket at man som registrert har rett til innsyn og rett til å bli glemt. Dette er eksempler på personvernkrav som ikke dekkes av informasjonssikkerhet alene.

   På den annen side avhenger personvern av informasjonssikkerhet, fordi det må være beskyttelse rundt lagring og behandling av personopplysninger. Nødvendige sikkerhetstiltak må være på plass for å sikre bl.a. konfidensialitet.

10. Ingen fasit. En fin video å se om dette er videoen i ressursbanken (https://www.uio.no/studier/emner/matnat/ifi/IN1020/h22/ressurser/Datasikkerhet/) om end-to-end encryption i whatsapp (https://www.youtube.com/watch?v=CINVwWHlzTY).

11. Case-oppgave:

    Alle sider av informasjonssikkerhet må vurderes, men spesielt konfidensialitet, integritet, autentisitet og sporbarhet (etterprøvbarhet).

    Skal alle alltid ha tilgang til all informasjon selv om man jobber på samme prosjekt? Hvis alle kan bruke en ulåst pc vet man ikke hvem som har endret/lagt til/slettet informasjon. Hvilke konsekvenser vil dette få, og for hvem? (Arbeidsplassen, deg selv, andre brukere) Kan du få problemer dersom en kollega bruker din pc til å utføre handlinger som ikke er tillatt? F.eks. spre informasjon som ikke skal spres, laste ned filer ulovlig eller utført andre handlinger i strid med intern sikkerhetsinstruks.

12. Case-oppgave:

    (a) Konfidensialitet, journalene inneholder sensitive personopplysninger. Integritet er også svært viktig, da en lege må kunne stole på at opplysninger om f.eks. allergier er korrekte. Autentisitet (ektehet), at alle parter kan stole på at identiteten og ekteheten til både brukere og system(er) er korrekt. Tilgjelgelighet er selvfølgelig viktig, det samme er er sporbarhet og mulighet til å etterprøve hendelser for både å rette opp i feil, samt unngå at tilsvarende feil skjer igjen.

(b) At noen tilsiktet eller utilsiktet endrer en pasients opplysninger om allergier. Potensielt dødelige følger. At systemet er utilgjengelig i kritiske øyeblikk, pga. feil eller angrep utenfra. At noen får tak i og lekker konfidensielle (helse-)opplysninger.

13. Enklest er å tvinge bruker til å lage passord som er kompliserte nok med store og små bokstaver og spesialtegn av en viss lengde. Kan også ha 2FA via google, microsoft eller ID-portalen. Evt... andre idéer? Sikkerhetsspørsmål er ofte ikke så lurt (lett å social engineer-e) og SÆRLIG ikke med hint. Hvis man må ha sikkerhetsspørsmål og det spørres om hint bør man ikke skrive et faktisk hint, men skriv noe tull i stede.

14. Tilgangskontroll

    (a) Autorisering = å **spesifisere** tilgangrettigheter.

    Tilgangskontroll = å **håndheve** tilgangsrettigheter.

    Autorisasjon er altså det som gjøres når en bestemmelse (policy) om hvem eller hva som skal ha tilgang til en ressurs nedfelles. Autorisering defineres som det å spesifisere tilgangsrettigheter til dataressurser.

    Tilgangskontroll defineres som det å håndheve disse tilgangsrettighetene i et datasystem hver gang et subjekt (bruker, prosess, maskin, ol.) ønsker å utføre en handling (lese, endre, slette, etc) på et objekt (en ressurss, f.eks. datafil eller et dataprogram/tjeneste). Å skulle utføre tilgangskontroll for kombinasjonen subjekt, handling, ressurs vil dermed kreve at subjektet er autentisert (vi vet hvem det er), og at forespørselen kan kontrolleres mot et forhåndsbestemt regelverk (autorisasjonen, policyen) og enten godkjennes eller avvises.

    (b) Noen eksempler på tenkelige (men ikke nødvendigvis ønskelige!) handlinger:

    - Student ønsker å levere en oppgave
    - Student ønsker å se en medstudents innlevering
    - Student ønsker å se tilbakemelding
    - Retter vil laste ned en students oppgave
    - Retter vil slette en students innlevering
    - Retter vil godkjenne en students innlevering

    (c) For å implementere policyer for autorisasjon i et datasystem er det nødvendig med tilgangskontroll. Tilgangskontroll krever autentisering, samt et system/program/applikasjon som har som oppgave å kan kontrollere og enten godkjenne eller avvise en forespørsel fra et subjekt om å utføre en gitt handling på et objekt.

15. Behandling av data: Praktisk oppgave, intet løsningsforslag.