IN1020 - Operativsystemer og datasikkerhet: Løsningsforslag gruppetime 5 (uke 39)

1. Operativsystemer:

   (a) Hvorfor har vi operativsystemer?

      i. Portable programmer, som fungerer på datamaskiner med forskjellig maskinvare. Det gjør at det blir enklere å forholde seg til.

      ii. Abstrahere bort maskinvaredetaljer. Detaljer om hvordan lagre filer? Hvordan sende data til nettverket? Hvordan bruke grafikkort.

      iii. Deling av ressurser mellom tjenester og programmer som kjører (scheduling, allokering). Operativsystemet sørger for rettferdig fordeling av tid mellom prosesser, tjenester og programmer.

      iv. Sikkerhet. Programmer skal ikke kunne se og forandre hverandres minneområder.

   (b) Hvor finner vi operativsystemer? Dette er noen av stedene hvor det finnes: datamaskiner, biler, smarte enheter (IoT), konsoller, mobiler, Nesten alle digitale enheter har et operativsystem, selv om de i mange tilfeller kan være veldig enkle.

   (c) Hvilke to perspektiver bruker vi for hva et operativsystem er?

      i. Extended machine (utvidet maskin): Gjemmer unna detaljene om maskinvare slik at den blir enklere å bruke å bruke datamaskinen

      ii. Resource manager (Ressurshåndterer): Deler ressursene mellom programmene som kjører på datamaskinen.

2. Hvilke hovedkomponenter finner man i et operativsystem?

   (a) Filhåndtering

   (b) Brukergrensesnitt (grafisk og tekst)

   (c) Prosesshåndtering

   (d) Enhetshåndtering (Device management)

   (e) Kommunikasjon (Internt mellom programmer og over datanettverk)

   (f) Minnehåndtering (allokering, aksess)

3. 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.

4. Se over

5. Se over

6. "Internet of Things (IoT)":

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

7. Samfunnskritisk infrastruktur:

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

8. 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.

9. Operativsystem og sikkerhet. Her er noen av momentene man kan være innom:

   Operativsystemet kar et klart skille mellom «user mode / brukermodus» og «kernel mode / kjernemodus».

   Vanlige programmer kjører i brukermodus, og har da begrenset tilgang til prosessoren, samt kan kun se sitt eget minne. Interne komponenter i operativsystemet kjører i kjernemodus har vil da kunne kjøre alle typer instruksjoner på prosessoren og se hele minne.

   Det er innebygd maskinvare i alle prosessorer som sørge for at disse modellene håndheves. Man bør derfor være veldig forsiktig med å gi programmer man ikke kjenner til tilgang til kjernemodus. (sudo på Linux eller Administrator på Windows)

   Snakk eventuelt i gruppen om noen har hørt om noe i media hvor noen har brukt sikkerhetshull i operativsystemet for å få tilgang til maskiner/data.

10. 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.

11. 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.

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