IN1020 - Nettverkskommuniksjon og datasikkerhet: Øvingsoppgaver gruppetime 2 (uke 36)

1 Sikkerhet

1. Brukerautentisering: Passord som autentiseringsfaktor.

   (a) Hva er et godt passord? Diskuter.

   (b) Hvordan bør vi håndtere og oppbevare passord? Er det f.eks. ok å skrive dem ned? Reflekter og diskuter.

   (c) Gjenbruk av passord: Det fleste av oss har så mange brukerkontoer ulike steder at det er fristende å gjenbruke samme passord flere steder. Diskuter hvorfor/hvorfor ikke dette er lurt.

   (d) "Passord som autentiseringsfaktor overlater ansvar for sikkerheten til brukeren". Hva tror du ligger i dette utsagnet?

2. Reflekter og diskuter: Ta for deg noen av brukerkontoene du har for ulike IT-tjenester, sosiale medier, nettbutikker, streamingtjenester, etc. (listen laget du kanskje i forrige ukes oppgaver), og tenk gjennom hvilke autentiseringsfaktor(er) du bruker de ulike stedene. Er brukerkontoene sikret god nok mot ID-tyveri? Er det noen tjenester du mener bør sikres bedre enn andre?

3. Du skal kjøpe (rådyre) pensumbøker på Akademika, og bruker et bankkort i kassa for betaling. Hva er egentlig identifikator og autentifikator for et bankkort? Hva identifiserer det? Og brukes 2FA? Diskuter :-)

4. Tilgangskontroll:

   (a) En vanlig misforståelse er å blande begrepene autorisasjon (authorization) og tilgangskontroll (access control). Repeter og vær sikker på at du forstår forskjellen.

   (b) Tilgangskontroll i Devilry: I innleveringssystemet *Devilry* som vi bruker på Institutt for informatikk har en bruker ulike roller i de ulike emnene (f.eks. i IN1020): Student, retter, faglærer og administrator. Studenter (som dere) skal/kan laste opp og leverer inn oppgaver, rettere (ofte gruppelærere) retter innleveringene og gir tilbakemeldinger til studentene, faglærer legger til rette for innlevering og administratorer har full oversikt over absolutt all informasjon i stystemet. Tenk deg fram til og gi eksempler på subjekt, objekt og handling i systemet Devilry. Ikke bind deg til handlinger du tror er tillatt!

   (c) forrige deloppgave beskriver i grove trekk hva de ulike rollene skal kunne gjøre og ha tilgang til i Devilry, med andre ord en policy for tilgang i Devilry. Datasystemet Devilry må dermed sørge for at disse policyene ivaretas/implementeres. Fortell kort om de overordnede mekanismene som må være til stede i Devilry for at dette kan overholdes.

5. Trusler mot autentisering

   Hva kan gå galt i en *autentiseringsfase*, hvordan kan *autentiseringen* angripes og utnyttes av uvedkommende?

6. Trusler mot tilgangskontroll

   Hva kan gå galt i bruken av *tilgangskontroll*, hvordan kan *tilgangskontroll* angripes og utnyttes av uvedkommende?

7. Case-oppgave: Du er med i utvikling av en webapplikasjon, og tilgangskontroll til denne. Dere vil implementere brukerautentisering der brukere logger seg inn med e-mail og et selvvalgt passord. Du er bekymret for at brukerne deres ikke kommer til å utøve nettvett og vil velge svake passord. Hvordan kan dere gå frem for å hindre dette? Kan bruk av andre autentiseringsfaktorer eller -løsninger være nyttig?

8. Case-oppgave: Petter jobber i justisdepartementet. Han er veldig fornøyd med å få jobbe med deres nye satsningsområde, automatisert saksbehandling, de neste to årene. Han har fått beskjed om å bytte kontorplass fordi alle som jobber i prosjektet skal sitte samlet i et åpent landskap i øverste etasje. Samtidig som de flytter inn i landskapet får de utdelt nye PC-er. På disse er det et klistremerke med budskapet "Lås PC-en når du går fra den!". Petter husker at informasjonssikkerhetsansvarlig snakket om dette på nyansattkurset han deltok på for lenge siden, men har egentlig aldri forstått hvorfor han skal låse PC-en sin. Alle i landskapet jobber på det samme prosjektet.

   Hvorfor skal de egentlig låse PC-en sin?

9. Case-oppgave: En kjent sportsbutikk har sin egen nettside som inneholder nettbutikk og en kundeklubb. brukere kan ta del i kundeklubben ved å lage en profil. Brukerprofilene inneholder data slik som e-mail, navn, adresse og telefonnummer for rask betaling via vipps. I tillegg kan brukere få oversikt over tidligere kjøp de har gjort og samle poeng som kan gi dem rabatter på fremtidige kjøp.

   (a) Hvilke verdier kan dere identifisere i dette scenarioet?
   (b) Hvem/hva er mulige trusselaktører?
   (c) Hvilke sikkerhetsmål vil dere prioritere å gjøre tiltak for å ivareta, og hvorfor?
   (d) Kan dere tenke ut noen sikkerhetstiltak som vil ivareta disse målene?

10. Case-oppgave:

    Et stort spillutviklingsselskap er i full sving med sitt neste AAA spill i en populær serie (et høy profil-spill med høyt budsjett for utvikling og markedsføring). Selskapet involverer 500 ansatte gjennom hele utviklingsprosessen, som inkluderer mange mindre team der noen f.eks. jobber med ting slik animasjoner og andre programmerer ulike deler av spillet.

    (a) Hvilke verdier kan dere identifisere i dette scenarioet?
    (b) Hvem/hva er mulige trusselaktører? Hva kan gå galt?
    (c) Hvilke sikkerhetsmål bør prioriteres, og hvorfor?
    (d) Hvordan ville dere sikret selskapet mot det dere kom frem til i b)? Hvilke sikkerhetstiltak bør benyttes?

2 Datanettverk

1. Beskriv kort forskjellene mellom linjesvitsjing (circuit switched) og beskjedsvitsjing (message switched) nett. Hva ligner mest på Internett i dag?

2. Hva er en protokoll, og hvorfor trenger vi det i datakommunikasjon?

3. Hvilke nettverkstopologier er mest vanlige i dag?

4. Diskusjonsoppgave:

   Hvilke sikkerhetsutfordringer har de mest brukte nettverkstopologiene, og hvordan kan vi løse disse utfordringene?