TK2100

T-08

**Modeller, standarder, lover og penetrasjonstesting**

Notater:

* Sikkerhetspolicy er sett med regler som definerer Subjekter, Objekter , handlinger og tillatelser

1. **Hva er en sikkerhetsmodell?**

Sikkerhetsmodellen er en struktur som tas i bruk av organisasjoner for å sikre it systemer ved hjelp av tilgangsrettigheter for at en bruker skal utføre arbeidsoppgavene sine.

1. **Hva er «DAC» (Discretionary Access Control)?**

DAC er adgangskontroll der brukerene selv har lov til å avgjøre hvilke tillatelser som gjelder for egne filer.

1. **Hva er «MAC» (Mandatory Access Control)?**

Dette er det motsatte av DAC der brukeren ikke selv bestemmer rettighetene på filene og ressursene sine og alle sikkerhetsavgjørelsene foretas av en sentral policy administrator.

Et eksempel er OSX der apple har noen filer i mac maskinene brukerne ikke har rett til å bestemme rettighetene på de filene.

1. **Nevn og beskriv minst to ulike adgangskontroll-modeller**

Disse modellene er utviklet for å formalisere mekanismer som beskytter konfidensialitet og integritet for primært dokumenter i et datasystem.

De mest kjente modellene er Bell- La- Pudula (BLP) og Biba

BLP modellen har en klassisk tvungen adgangskontroll (MAC) modell for å beskytte konfidensialitet

Modellen er basert på det militære flernivå sikkerhetsparadigmet for dokumentklassifisering og personell klarering

Det er en streng lineær orden av brukernivåer for dokumenter og adgang

På norsk: Ugradert, begrenset, konfidensielt, hemmelig, strengt hemmelig

En bruker kan lese alle dokumenter på eget klareringsnivå og under (og kan ikke lese dokumenter i høyere sikkerhets nivå)

• En bruker kan ikke skrive til lavere nivå («forhindre lekkasje»), men en bruker på lavere nivå kan skrive oppover... (men brukeren som skrev dokumentet kan ikke lese av dokumentet som er sendt i høyere nivå)

• «Informasjonsendringer flyter bare oppover»

Biba ligner på BLP modellen , men har i oppgave å beskytte integritet fremfor konfidensialitet. Integritetsnivåene defineres for brukere og objekter for å skildre påliteligheten.

F.eks. vil en dokument lagret på sentraladministrert server vil typisk ha en høyere nivå enn sammenlignet med en vanlig laptop.

En mangåring ansatt har en høyere nivå enn nyansatt.

Reglene er det motsatte av BLP der lesing fra lavere nivå eller skriving til høyere ikke er tillatt.

Informasjonsendringene skal bare flyte nedover ikke oppover som i BLP.

1. **Hvordan ser sikkerhetsprosessen ut?**

Sikkerhetsprosessen ser slik ut:

1. Vurdere risiko: Verdier, trusler, tap

2. Utforme policy: Informasjon, systemer, bruk, backup,

tilgang, hendelser, avbruddsplan

3. Innføre: Rapportering, autentisering, innbrudds-

deteksjon, kryptering, fysisk sikkerhet.

4. Opplæring: Ansatte, ledere, utviklere, sikkerhets-

ansatte

5. Revisjon: Etterlevelse, periodisk vurdering,

innbrudds-testing

1. **Beskriv «Standard: ISO 27000»**

Standard ISO27000 beskriver oppbygningen og vedlikehold av et Information Security Management System (ISMS) for et foretak. ISO27000 er en internasjonal tittel, som har et fokus på sikring av tilgjengelighet, integritet og konfidensialitet. Sikringen foretas via et sett kontroller , som angir konkrete krav . Kontrollene beskrives og vedlikeholdes i organisasjonen. ISO 27000 kan opprettholdes og dokumenteres gjennom en

sertifiseringsordning, og kontrolleres gjennom en intern og en ekstern revisjon

1. **Hva er «PCI DSS»?**

**Det står for Payment Card Industry Data Security Standard**

Dette er standarden som betalingstjenestene bruker som f.eks. Visa, MasterCard og stiller krav til sikring av kunde, leverandører og transaksjoner. Dette må sertifiseres og revideres etter denne standarden dersom du skal f.eks. drive en nettbutikk , serverfarm for en bank eller andre tjenester som benytter seg av betalinger

1