Informasjonssikkerhet: Teori og praksis

Audun Jøsang
2. utgave 2023
Universitetsforlaget

Oppgaver

Kapittel 9: IAM – Identitets- og tilgangshåndtering

Oppgave 1: IAM-begreper

a. Gi en kort forklaring på følgende begreper knyttet til identitetshåndtering.
   (i) Entitet
   (ii) Identitet
   (iii) Bruker-ID (identifikator, entydig navn)
   (iv) Digital identitet
   (v) Autentikator
b. Forklar kort hva som menes med begrepet "identitets- og tilgangshåndtering" IAM.

Oppgave 2: Silo-modell og føderert modell

a. Beskriv kort silo-modellen for identitetshåndtering.
b. Beskriv fordeler og ulemper ved silo-modellen.
c. Beskriv generelt den førderte modellen for identitetshåndtering.
d. Beskriv fordeler og ulemper ved den førderte modellen.

Oppgave 3: ABAC – Attributtbasert tilgangskontroll

Attributtbasert tilgangskontroll, eller ABAC (Attribute-Based Access Control) er en fleksibel modell for tilgangskontroll.

a. Nevn fire kilder for attributter i ABAC.
b. Forklar hvordan DAC kan implementeres med ABAC.
c. Forklar hvordan MAC kan implementeres med ABAC.
d. Forklar hvordan RBAC kan implementeres med ABAC.

Oppgave 4: IAM faser og trinn

a. Tegn et diagram av IAM i form av to faser, med et sett med trinn, og angi hvilke trinn som tilhører identitetshåndtering (Identity Management) og hvilke trinn som tilhører tilgangshåndtering (Access Management).
b. *Autorisering* er et essensielt begrep i ISO 27000 sine definisjoner av konfidensialitet, integritet og tilgjengelighet. Dessverre blir autorisering ofte beskrevet på en måte som er inkonsistent med ISO 27000. Gi en (i) konsistent (riktig) og (ii) inkonsistent (feilaktig) tolkning av begrepet autorisering relatert til de to fasene i IAM.

Oppgave 5: Sentralisert og distribuert ID-føderering

Føderert identitetshåndtering kan ha sentralisert eller distribuert autentisering, og kan ha sentralisert eller distribuert navnerom. Finn typiske eksempler på forskjellige ordninger for føderert identitetshåndtering som brukes, og se hvor de passer inn tabellen nedenfor, og forklar på hvilken måte de er sentralisert eller distribuert. Vurder e, g, Aadhaar (Indias «unique identity»), det tyske eID, Eduroam, FEIDE, ID-porten, HelseId, europeisk eID, internett-IdP-ene facebook/google/twitter/apple/microsoft, og andre som du kommer på.

	Sentralisert navnerom	Distribuert navnerom
Sentralisert autentisering		
Distribuert autentisering		

Oppgave 6: Kommersiell og militær tilgangshåndtering

a. Hvilke modeller for tilgangskontroll er tradisjonelt brukt i
    i. Kommersielle systemer
    ii. Militære systemer
b. Hvilket er det viktigste sikkerhetsmål som MAC (Bell-LaPadula) støtter?
c. Gi et eksempel på et anvendelsesområde der MAC (Bell-LaPadula) er hensiktsmessig.
d. Forklar kort følgende sikkerhetsprinsipper i Bell-LaPadula:
    (i) «No read up» (simpel security property: SS),
    (ii) «No write down» (Star property: *)
e. Anta at en bruker har sikkerhetsklarering STRENGT HEMMELIG. Hvordan kan brukeren redigere (lese og skrive) et dokument som har en lavere sikkerhetsgradering, f.eks. HEMMELIG?

Oppgave 7: Distribuert tilgangsstyring

a. Hva var internettindustriens motivasjon for å utvikle OAuth-standarden?
b. Hvordan kan OAuth benyttes for tilgangsstyring for tilgang mellom virksomheter inne en sektor, f.eks. for tilgang til pasientdata innen helsesektoren.