IN2120 – Informasjonssikkerhet: Workshop uke 1

Oppgave 1

1. i. Konfidensialitet: The property that information is not made available or disclosed to unauthorized individuals, entities or processes.

NO: Den egenskapen at informasjon ikke er gjort tilgjengelig eller avslørt til uautoriserte individer, enheter eller prosesser.

Integritet: The property that data has not been altered or destroyed in an unauthorized manner.

NO: Den egenskapen at informasjon ikke har blitt endret eller ødelagt på en uautorisert måte.

Autorisering: The granting of rights, which includes the granting of access based on access rights.

NO: Tildelelsen av rettigheter, inkludert tildelelsen av tilgang basert på tilgangsrettigheter.

Ja, fordi autorisering handler om å gi rettigheter og tilgang basert på hvem som har tilgangsrettigheter, og konfidensialitet blir på denne måten overholdt gjennom at informasjonen ikke skal gjøres tilgjengelig uten tilgangsrettigheter/autorisasjon. Integritet handler på samme måte om at uautoriserte uten tilgangsrettigheter ikke skal kunne endre eller ødelegge informasjon.

ii. Ja, “Computer Fraud and Abuse Act” er meningsfull I forhold til hvordan autorisering er definert, ved at man git rettigheter og tilgang basert på hvem som har tilgangsrettigheter/er autorisert.

iii. Autorisering er en tildeling av rettigheter til tilgang på informasjon, som sikrer integritet og konfidensialitet, og søker å hindre informasjon fra å bli misbrukt av uvedkommende.

1. (Mangler læreboka) s. 733, figur 5-2 og tekst i 2. og 3. avsnitt.
2. «Autorisering» er definert på wikipedia som «en funksjon som spesifiserer tilgangsrettigheter/privilegier til ressurser, relatert til informasjonssikkerhet og datasikkerhet generelt og adgangskontroll spesielt.». «Å autorisere er å definere en tilgangs-policy (retningslinjer for å oppnå bestemte mål.»
3. ?

Oppgave 2

1. Relevante trusler mot trinnene i **konfigurasjonsfasen** av IAM (identitets- og tilgangshåndtering):

* Brukeren registreres med feil navn.
* Brukeren er riktig registrert, men akkreditivene (passord eller brikke) sendes til feil person.
* Riktig registrering og klargjøring av akkreditiver, men det konfigureres altfor vid tilgangsautorisasjon, som ikke er i samsvar med autorisasjonspolicyen som gjelder for jobbrollen.

1. Potensielle trusler mot **driftsfasen** av IAM:

* Passord kan gjettes fordi svake passord er tillatt, eller at det ikke finnes begrensninger for antall forsøk, slik at falsk innlogging er mulig.
* Biometrisk autentisering kan manipuleres på grunn av svak beskyttelse mot presentasjonsangrep (f.eks. gummifinger, eller å vise bilde av ansikt).
* Uautorisert tilgang til ressurser, fordi regler for tilgangskontroll ikke håndheves konsekvent og sikkert av systemet.

Oppgave 3

1. Sårbarheter som hovedsakelig er utnyttet av phishing-angrep er sårbarheter hos mannesker, som uvitenhet, godtroenhet og dårlig oppmerksomhet/bevissthet.
2. Mulige sikkerhetstiltak for å forhindre eller mitigere phishing-angrep kan være bevisstgjøring for å gjøre folk i stand til å oppdage når avsenderen er en angriper som gir seg ut for å være en legitim avsenderr, eller kunne oppdage falske e-postmeldinger basert på innholdet. Tekniske tiltak må være i form av praktiske sikkerhetsmekanismer for å oppdage phishing-angrep, for eksempel ved å filtrere e-post etter innhold eller andre aspekter, eller ved avsender-autentisering.

Oppgave 4

Sikkerhetspolicy for min personlige laptop, som uttrykker hvem som er autorisert til å få tilgang til å bruke den:

Ettersom jeg er eier av denne laptopen, er kun jeg autorisert til å bruke den. På samtykke fra meg, kan jeg autorisere en bestemt annen person til å bruke min laptop, når jeg gjennom brukerautentisering låsen den opp, og under mitt tilsyn lar personen få tilgang til Internett via en nettleser på laptopen. Til enhver tid kan jeg tilbakekalle autorisasjonen ved å si dette til personen, som da gjør at personens bruk av min laptop må opphøre med det samme.

Oppgave 5

1. Meldingskonfidensialitet/Forbindelsesløs konfidensialitet:

Meldingskonfidensialitet/forbindelsesløs konfidensialitet kan oppnås gjennom kryptering og ruterkontroll.

* Kryptering betyr at dataene er kryptert, og derfor uleselig for angripere som ikke kan dekryptere.
* Rutingkontroll betyr at datapakkene rutes gjennom beskyttede nettverk (f.eks. kabler) hvor ikke-autoriserte parter ikke fysisk får tak i signalene.

1. Meldingsintegritet/Forbindelsesløs integritet kan oppnås gjennom kryptering, digital signatur og dataintegritet.

* Kryptering gjør det umulig for angripere å endre eller lage falske meldinger uten å bli oppdaget.
* Digital signatur og dataintegritet (MAC/Meldingsautentiseringskode) betyr at en kryptografisk sjekksum sendes sammen med den opprinnelige meldingen, som kan bekreftes av mottakeren, slik at angripere ikke kan endre eller lage falske meldinger uten å bli oppdaget fordi sjekken på mottakersiden vil mislykkes. Men en angriper kan slette en melding uten å bli oppdaget.

Oppgave 6

Brukerautentisering gir relativt lav forsikring om data/meldingsautentisitet. Det er en mulighet for at brukeren har forlatt pcen uten å låse den, for eksempel for å ta en kaffe eller gå på toalettet, og at en annen person bruker pcen til å sende data til serveren. En annen mulighet er at klientcomputeren er infisert med en trojaner som genererer og sender data til serveren uten brukeren viten, selv om brukeren fysisk sitter foran pcen og aktivt utfører transaksjoner, for eksempel mot nettbanken.

Hvis økten mellom klient og server ikke er beskyttet med TLS (Transport Layer Security) eller noen annen VPN (Virtual Private Network)-teknologi, så er det en mulighet for at et mann-i-midten-angrep kan skje, som dermed kan endre eller slette data som utveksles mellom klienten.

**Oppsummering:**

Brukerautentisering gir nokså lav forsikring om meldingsautentisitet, siden det er en mulighet for at en annen har fått tilgang til pcen fysisk eller gjennom å infisere pcen med en trojaner som sender data til serveren. Dersom økten ikke er beskyttet med en VPN, for eksempel TNS, er det en mulighet for at et mann-i-midten-angrep kan skje, hvor data kan bli endret, slettet eller utvekslet.

Oppgave 7

1. Personopplysningsvern krever for eksempel forebygging av uautorisert innsamling og lagring av personlige opplysninger, som ikke dekkes av KIT-egenskaper.
2. Personopplysningsvern avhenger av informasjonssikkerhet fordi det må være tilstrekkelig beskyttelse rundt lagring og behandling av personopplysninger.