T-00

**INTRODUKSJON**

# Hva er informasjonssikkerhet?

Informasjonssikkerhet handler om å sikre informasjon og sørge for at den ikke kommer ut til uvedkommende og at informasjonen ikke blir endret utilsiktet eller av uvedkommende(svindlerne) samt at informasjonen er tilgjengelig i forhold til behovet. «Sikkerhet er alltid i forhold til trusselbildet»

**Informasjonssikkerhet handler om å sikre informasjon slik at den ikke faller i hendene til en svindler eller uvedkommende og at informasjonen ikke endres av uvedkommende eller helt tilfeldig(utilsiktet). I tillegg skal informasjonen være tilgjengelig etter behov.**

# I forhold til informasjonsikkerhet hva står «C.I.A» for?

Det står for Confidentiality (konfidendsialitet) , Integrity(Integritet) , Availability (tilgjengelighet)

Alle må oppfylles for å være et sikkert datasystem

Konfedensialitet: Adgangskontroll

# Forklar begrepene nedenfor (gi gjerne eksempler på begrepene også):

* + **Kryptering**

**Går også ut på det vi gjør med dataene**

**Kryptering er en måte å la to parter kommunisere over en usikker kanal, som for eksempel kan overvåkes. Hvis informasjonen er kryptert så er den eller skal være sikker slik at den ikke overvåkes.**

◦ En måte der man kan la to parter utfører konfidensiell (privat) kommunikasjon over en usikker kanal som for eksempel kan overvåkes. Informasjonen skal dermed være sikker fordi den er kryptert

# Adgangskontroll

# Det er regler og retningslinjer som brukes om å begrense adgangen til konfidensiell informasjon til de personene eller systemene som behøver å vite det («Need to Know)». Dette gjelder både datasystemer og personer

# ◦ Regler og retningslinjer som begrenser adgangen til konfidensiell informasjon til de personene/systemene som «trenger å vite»(«need to know»). Dette gjelder både personer og datasystemer.

# Autentisering

# Avgjør rollen eller identiteten til noen (person). Det finnes flere ulike måter å gjøre dette på , og det kan f.eks. være passord, bilnøkler, telefon, fingeravtrykk , smartkort.

# Å avgjøre identiteten eller rollen en person har, eksempler kan være passord, bilnøkkel, fingeravtrykk o.l.

# Autorisering

# Autorisering avgjør hvilke ressurser en person/system skal ha tilgang til. Et eksempel på det er låste dører der personen med nøkkelen har tilgang til.

* Å bestemme hvilke ressurser en person/system skal ha tilgang til. Eksempler på autorisering kan være låser på dører der bare personen med nøkkel har tilgang.

# Hva betyr Integritet? Hvordan kan man bevare integriteten til noe?

Integritets handler om at informasjonen ikke har blitt endret på en uautorisert måte. Ulike måter man kan bevare integritet på kan være for eksempel backup og sjekksommer

# Hva betyr Tilgjengelighet?

# Går ut på at informasjonen er tilgengelig og man har mulighet til å endre innenfor en rimelig tid av de

# • Tilgjengelighet handler om at informasjonen er tilgjengelig og mulig å endre innenfor en rimelig tid av de som er autorisert til dette.

# Hva står begrepet «A.A.A» for? forklar kort hva hver enkelt «A» står for.

# • Assuranse(forsikring/tillit)

# ◦ Forventet atferd, hva som er tillat og hvilke mekanismer som benyttes for å håndheve retningslinjer.

# • Autentisitet

# ◦ Måten man kan bestemme om utsagn, retningslinjer og tillatelser som blir gitt av en person eller et system er ekte.

# • Anonymitet

# ◦ Anonymitet handler om at transaksjoner eller lagrede data ikke skal kunne føres tilbake til et bestemt individ.

# Er Cæsar Chiper en «sikker» måte å kryptere informasjon på? (bytter en bokstav med en annen A krypter gir D,B gir E ,C gir F ,E gir G osv.

* + Ja
  + **Nei (Den er sårbar for frekvesanalyse)**

# Hva slags kryptografiske funksjoner er: «SHA-1» og «SHA-256» eksempler på?

* + Dette er ikke kryptografiske funksjoner
  + **Dette er Hash funksjoner**
  + Dette kan man ikke svare på uten å vite hvilken algoritme klokkesyklusen på en datamaskin kjører.

# Hva står «MAC» for?

* + Message Autorization Certificate
  + **Message Authentication Codes**
  + Message Anonymity Controll
  + Ingen av alternativene

# Hva vil et «DOS» angrep bety?

# Det står for Denial-of-service og DOS angrep defineres ved å avbryte eller forhindre en datatjeneste eller ødelegge tilgangen.

* + Denial-of-service angrep betyr å avbryte eller forhindre en datatjeneste eller ødelege tilgang. .

# Nevn de 10 prinsippene for sikker design av datasystemer og en kort beskrivelse av hver av de.

* + Economy of mechanism

Det er et enkelt mulig design og implementering av sikkerhets-tiltak slik at andre kan forstå, videreutvikling, og verifisering effektiviseres. Dette gjelder programvareutvikling

Enkelt mulig design og implementering av sikkerhets-tiltak sånn at andre

◦

lettere kan forstå og videre utvikling og verifisering effektiviseres.

* + Fail-safe defaults
  + Er standard konfigureringer som forholder seg til konservative beskyttelses-skjema(er) .OS og applikasjoner prioriterer ofte brukervennlighet over sikkerhet «Det er bedre å gi for lite tilgang enn for mye»

Standard konfigureringer som følger konservative beskyttelses-skjema(er).

◦

«Bedre å gi for lite tilgang enn tilgang til for mye»

* + Complete mediation

Sjekker all tilgangen til en ressurs og sørger for at det er i linje med beskyttelses-skjema. F.eks. automatisk utlogging etter en viss periode.

Sjekke all tilgang til en ressurs og passe på at det er i tråd med beskyttelses-

◦

skjema. For eksempel automatisk utlogging etter en viss periode

* + Open design

Burde dele arkitektur og design for at andre parter kan undersøke og

◦

analysere systemet. Eneste som ikke burde deles er de kryptografiske nøklene.

* + Separation of privilege

Man må kunne få tilgang til en del av systemet uten at man får tilgang til

◦

hele systemet. Systemet må også kunne kreve at flere ulike betingelser er innfrid for å få tilgang til ressurser eller at et program skal utføre en bestemt handling.

* + Least privilege

Hvert program bør operere med kun det minimum av rettigheter det trenger

◦

for å fungere skikkelig. Opperere med «need to know» prinsippet for deling av informasjon.

* + Least common mechanism

I systemer med flere brukere bør mekanismer som tillater deling av en

◦

ressurs mellom flere brukere minimeres.

* + Psychological acceptability

Bruker-grensesnitt og tilbakemeldinger bør være godt designet og

◦

«intuitive» samt alle sikkerhets-innstillinger bør være i tråd med hva en

«vanlig bruker» forventer.

* + Work factor

Kostnadene ved å måtte omgå/bryte en sikkerhets-mekanisme bør

◦

sammenlignes med de ressursene en forventet angriper vil disponere. Dette vil dermed si at et system som skal beskytte for eksempel karrakterene til studenter der ofte studentene er angripere ikke trenger å være like

sofistikert/avanser som et system som skal beskytte atomvåpen, statshemmeligheter eller industrihemmeligheter.

* + Compromise recording
    - Noen ganger er det bedre å få oversikt(loggføre) konsekvensene av et inngrep enn å sette inn mer sofistikerte tilgang for å forhindre det.

Eksempler kan være overvåkningskamerea i stedet for å sikre alle dører of vinduer bedre.