

SIKKERHET

Shahi Ftah
Gruppe 13
shahiaf@uio.no

Hva er sikkerhet?

- Trygghet og visshet, forebygging av uhell
- Beskyttelse mot alt uønskede
- Definisjon:

«Sikkerhet kan defineres som en tilstand; fravær av uønskede hendelser eller frihet fra fare og frykt» Tilstanden påvirkes av endringer som trussel og farer, sårbarhet og verdi.

Beskytte verdier mot skadelig hendelser

Hva som kan utgjøre en trusselen og hvilke trusler må man holde seg til



Sikkerhet

Mange grener fra sikkerhet:

- Datasikkerhet
- Cybersikkerhet
- Nettverkssikkerhet
- Informasjonssikkerhet

I praksis betyr alle det samme, men deres popularitet har endret seg



Sikkerhetsmål

En egenskap man kan ønske å oppnå eller tilby

Noe man retter frem mot å ha oppnådd

Definisjon:

Beskyttelse av informasjonens Konfidensialitet, Integritet og Tilgjengelighet.

I tillegg kan andre egenskaper, f.eks. autentisitet, sporbarhet, ubenektelighet, personvern og pålitelighet omfattes. (ISO/IEC 27000:2018

Sikkerhetsmål

- K- Informasjonen ikke tilgjengeliggjøres for annet en de som er autorisert for tilgang
- I- Stole på at data ikke er slettet eller endret uautorisert
- T- Info er tilgjengelig til enhver tid for den som har tilgang

- Autentisitet – Du er personen som du utgir for å være
- Sporbarhet – Hvem har utført handlingene?
- Uavviselighet – Bekrefte at data er sendt og mottatt
- Personvern – Sikre dine data og dine rettigheter til bruk



Autentisitet

- Autentisitet bekrefter identitet:
- Brukerautentisering
- Organisasjonsautentisering
- Systemautentisering
- Dataautentisering

- Men hvordan kan vi stole på at brukeren er autentisk?
- Autentiseringsfaktor – Noe du vet, noe du har, noe du er
- Flerfaktor-autentisering



Sikkerhetstiltak

- Gjøre noe for å oppnå sikkerhetsmålene
- Deles i 3 grupper:

Organisatoriske tiltak
- ISMS/Styring/Ledelse
- Policyer/Standarder
- Hendelseshåndtering
- Personellsikkerhet
- Sikkerhetskultur
- Øvelser
- etc.

Fysiske tiltak
- Kameraovervåking
- Adgangskontroll
- Skjerming av kabler
- Vektere
- Låser
- Alarmer
- etc.

Teknologiske tiltak
- Brukerautentisering
- Tilgangskontroll
- Systemsikkerhet
- Nettverkssikkerhet
- Sikkerhetskopiering
- Kryptering
- etc.

Sikkerhetsmål:

Konfidensialitet – Integritet – Tilgjengelighet

støtter

Sikkerhetstiltak:

f.eks. låser – kryptering – autentisering - sikkerhetskultur

Verdier og Trusler

- *Hva er en verdi?*
- Informasjonsressurser. Målet er å beskytte verdienes KIT
- *Trussel:* Ønsker å oppnå verdiene, som potensielt kan skade f.eks. organisasjonens verdier.
- *Sårbarheten:* manglende sikkerhetstiltak og evne til å håndtere

- Hvem er trusselen?
- Hvis jeg har tilgang til en ressurs, er jeg da autorisert til ressursen?

Hva med deg?

- Behandling av personopplysninger
- Rett til privatliv
- Rett til innsyn
- Rett til å bli glemt

- Hva om vi blir hacket?
- Passord knekkes?
- Alle spor loggføres som er en bidrag til sporbarhet
- Planlegge katastrofe - Sikkerhetskopier



Sikkerhetsmål

Sikkerhetsmål er et sentralt begrep innen informasjonssikkerhet. Hvilke av følgende defineres som sikkerhetsmål:

Velg ett eller flere alternativer

 Integritet

Autorisering

 Uavviselighet

Brannmur

 Tilgjengelighet

Orm

Tilgangskontroll

Tofaktor-autentisering

Trusselmodellering

Hvorfor kan bruk av USB minnepinner utgjøre en *sikkerhetstrussel* mot sikkerhetsmå konfidensialitet?

Velg ett eller flere alternativer

- [ ] De kan utilsiktet bli kryptert av for eksempel løsepengevirus.
- [ ] De kan bringe med seg skadevare som omgår andre sikkerhetsmekanismer.
- [ ] De kan bruke for mye strøm og på den måten påvirke en datamaskin negativt.
- [ ] De kan stjeles.