IN1020 - 9. gruppetime

Dagens agenda

Første time:

- Rask repetisjon
- Cyber Awareness Challenge?

Andre time:

- Ukeoppgaver
- Pilotarbeid

Verdier

Hva som er en verdi handler om *hva som er viktig for noen i et gitt tilfelle.*

- Hva er viktig for deg?
- Hva er viktig for en virksomhet?
- Hva er viktig for samfunnet?

Dataangrep

En tusselaktør er…

den som kan tenkes å utføre en potensielt skadelig handling.

Men *hvem er* trusselaktørene?

- Sporadiske «hackere»
- Aktivister
- Kriminelle
- Virksomheter
- Nasjonalstater

Sikkerhetsmål

KIT

- **Konfidensialitet**: Å sikre at ingen andre enn de med rettmessige behov har tilgang til informasjon.
- **Integritet**: Å sikre at informasjon alltid er korrekt, og ikke endres eller slettes utilsiktet.
- **Tilgjengelighet**: Å sikre at en informasjon alltid er tilgjengelig for rett person til rett tid.

Autentisitet

- **Autentisitet**: Hvor sikre er vi på at noe eller noen er det/den de utgir seg for å være?

- Autentisitet er interessant i flere sammenhenger:
  - for en **bruker**
  - for et **system** eller en **organisasjon**
  - for opprinnelsen til **data**

Uavviselighet

- **Uavviselighet**: Hindre mulighet for *fornektelse* av at data er sendt eller mottatt, også ovenfor en 3. part.
  - Uavviselig *opphav*: Bevis for at data er sendt
  - Uavviselig *mottak*: Bevis for at data er mottatt
- Krav om uavviselighet skaper behov for et «bevis» som kan bekreftes eller avkreftes av en tredjepart.
- Det vi kaller en *digitale signatur* er en variant av et slikt bevis.

Sporbarhet

- **Sporbarhet**: Å kunne knytte en gitt identitet til en gitt hendelse.
- Sporbarhet i IT-systemer ivaretas gjennom å
  - Identifisere alle identiteter
  - Loggføre alle hendelser
  - Analysere/etterforske

- Disclaimer:

Ved datainnbrudd vil en angriper mest sannsynlig forsøke å fjerne alle spor.

Sikkerhetstiltak

Fysiske tiltak

Eksempler:

- *Gjerde/dør*
- *Lås*
- *Overvåkning*
- *Fysisk tilgangskontroll*

Teknologiske tiltak

Eksempler:

- *Digital tilgangskontroll*
- *Autentiserings-mekanismer*
- *Sikkerhetskopiering*
- *Sikkerhetsoppdatering*
- *Kryptografi*

Administrative tiltak

Eksempler:

- *Opplæring*
- *Retningslinjer*
- *Prosedyrer*
- *Hendelseshåndtering*

Autentisering

Å bekrefte en hevdet identitet.

Former for autentisering:

- Organisasjonsautentisering (*organization authentication*)
- Systemautentisering (*system authentication*)
- Autentisering av dataopprinnelse (*data-origin authentication/ message authentication*)
- Brukerautentisering (*user authentication*)

Autorisering

«Å autorisere er å godkjenne eller gi løyve»

- Å autorisere er å spesifisere en *tilgangs-policy*.
- Autorisering er altså **ikke** teknologi, men policy.
- Eksempel på en slik policy:
  «En ansatt i lønnsavdelingen skal ha tilgang til lønnssystemet.»

Tilgangskontroll

«Tilgangskontroll innebærer å sjekke om et subjekt har tilgang til å utføre en ønsket handling på et objekt, etter forhåndsdefinerte regler»

Eksempler på forespørsler fra *subjekter*:

- Anne vil lese innholdet i en fil
- Per vil oppdatere kontobalansen på en bankkonto
- En applikasjon vil opprette en nettverksforbindelse mot en annen maskin

Tilgangskontroll = autentisering + autorisasjon

Lagring av informasjon

Kryptering

- Å kryptere lagrede data er en strategi for å understøtte konfidensialitet og integritet
- **Mål**:
  - Å sørge for at informasjon ikke kommer uvedkommende i hende ved å gjøre data uleselig/uforståelig for utenforstående.
  - Å sørge for at modifikasjon av data oppdages.
  - Eksempel: Laptop mistes/stjeles, datainnbrudd på server/tjener der data lagres.

Utfordringer:

- Kryptering og dekryptering er ressurskrevende for datasystemer
- Krypteringsnøkkel på avveie

Sikkerhetskopi

- Sikkerhetskopiering er en strategi for å ta vare på informasjon over tid.
- **Mål**: Bidra til økt tilgjengelighet ved å være i stand til å gjenopprette systemer og data ved uønskede hendelser som endrer eller sletter informasjon.

Viktig ved sikkerhetskopiering:

1. Ta vare på *flere ulike versjoner* av informasjon.
2. Sikkerhetskopien må også sikres: Lagres trygt adskilt fra opprinnelige disker/data, utilgjengelig for uvedkommende.
3. Sikkerhetskopi =/= datasynkronisering

Informasjonsklassifisering

Åpen informasjon

Begrenset informasjon

Konfidensiell/ sensitiv informasjon

Nettverkssikkerhet

Sikkerhetstrusler

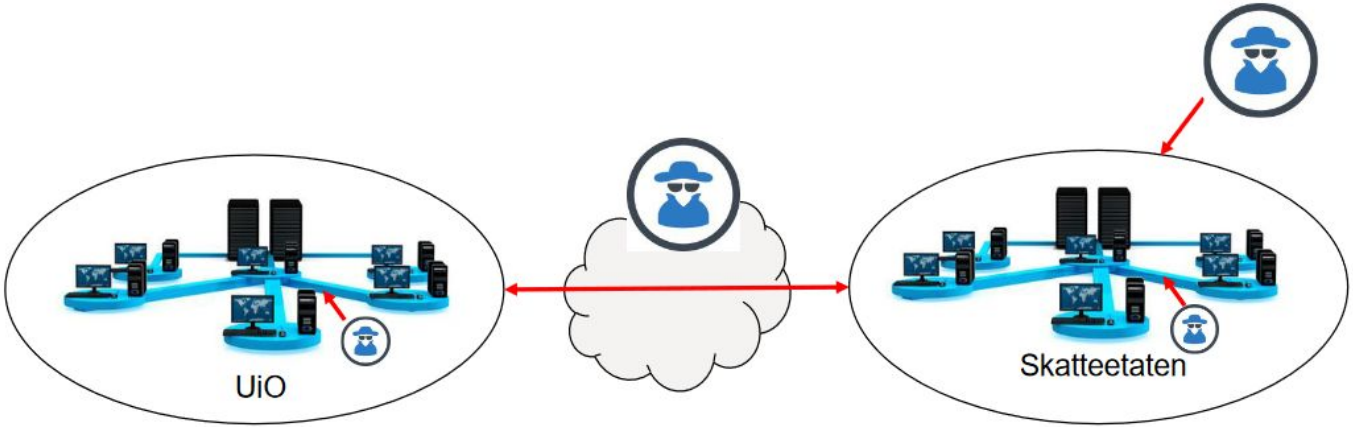
Trusler:

- På datatrafikk:
  - **Avlytting**: Uvedkommende lytter til nettverkstrafikk og får tak i konfidensiell informasjon. *Passivt angrep.*
  - **Data modifiseres** (Man in the Middle-angrep, MitM): Uvedkommende griper inn i kommunikasjonen og modifiserer data. *Aktivt angrep.*
  - **Forfalskning**: Uvedkommende sender ikke-autentiske meldinger eller later som de er en annen. *Aktivt angrep.*
- Tjenestenektangrep: Utilgjengelige ressurser
- Uautorisert bruk: Misbruk av ressurser

Berørte sikkerhetsmål:

- Konfidensialitet
- Integritet
- Autentisitet for opphav til data/melding.
- Tilgjengelighet

Nettverkssikring



Nettverkssikkerhet kan sies å bestå av følgende to hovedområder:

- Kommunikasjonssikkerhet: Beskytte data i transporten mellom virksomheter/endenoder.
- Skallforsvar: Beskytte en virksomhets dataressurser mot uautorisert tilgang fra omverdenen.

Skallforsvar

- **Brannmur**:
  - Slipper inn eller avvise trafikk inn i og/eller ut fra et nettverk basert på forhåndsdefinerte regelsett.
  - Brannmur fungerer som en *tilgangskontroll* for nettverket.
  - Kan være et dataprogram eller maskinvare laget for akkurat dette formålet.
- **Innbruddsdeteksjon**
  - Overvåker nettverkstrafikk, og kan detektere:
    - Både forsøk på og suksessfulle innbrudd
    - Datavirus og annen ondsinnet programvare
    - Tjenestenektangrep

Ukeoppgave case

Cyber Awareness Challenge

Ukeoppgaver

Pilotarbeid

Pause til 09:15

Takk for i dag! :)