

UiO : Institutt for informatikk

Datateknologi og sikkerhet

IN1020 – Introduksjon til datateknologi

18.11.2021

Kristin Skar
kritisk@ifi.uio.no

Pensum datasikkerhet

- Utvalgte kapitler og deler av kapitler fra læreboka «Datasikkerhet»
- Stoff gjennomgått på forelesningene.
- Alt av ukeoppgaver.
- Obligatorisk oppgave nr 1.
- Læringsmålene gitt på hver forelesning gir en god pekepinn for hva dere skal kunne.

Pensum: Heide/Nätt - Datasikkerhet

Heide/Nätt

«Datasikkerhet. Ikke bli svindlernes neste offer», 2. utgave:

Kap. 1, 2, 3, 4, 5 (s115-128 + s134-143), 6, 7 (s169-182 + s189-195), 13, 14 (kursorisk), 15 (s385-389)

(**Heide/Nätt – «Datasikkerhet. Ikke bli svindlernes neste offer», 1. utgave:**

Pensum er kapitlene 1, 2, 3, 4, 5 (s.109-131), 6, 7 (s.165-170 + 178-183), 8 (s.187-200 + 206-210), og 13.)

Eksamen

- ✓ Forventer en overordnet forståelse.
- ✓ Forventer at dere skal kunne anvende forståelsen i enkel trusselmodellering.
- ✓ Kjenne til typiske sårbarheter samt sikkerhetstiltak.
- ✓ Kjenne til personopplysningsvern og at personopplysningsvern er regulert i lovverk
- ✓ Kjenne til informasjonssikkerhetens rolle i virksomheter og organisasjoner.
- ✓ Detaljnivå som på forelesning/gruppetimer.

Datateknologi og sikkerhet

Cybersikkerhet

- Beskytte alt som er koblet sammen via internett.

Informasjonssikkerhet:

- Beskytte digital informasjon og verdier.
- Beskytte *informasjonsressurser*.

Sikkerhetsmål. Hva ønsker vi oppnå?

- **Konfidensialitet**
- **Integritet**
- **Tilgjengelighet**

Kjent som *CIA* (KIT)

- **Autentisitet**
- **Uavviselighet**
- **Sporbarhet**
- **Personvern**

Sikkerhetsmål: Autentisitet

Autentisitet til ulike entiteter, med ulike autentiserings-former:

Brukerautentisering, med autentiseringsfaktorer:

- «Noe du husker»
- «Noe du har»
- «Noe du er»
- To-faktor/multi-faktor

System- og organisasjons-autentisering

Autentisering av dataopprinnelse

Hvordan ivareta sikkerhetsmål? Innføre *sikkerhetstiltak*

For alle *datatilstander*

- Lagring
- Overføring
- Bruk

I ulike *faser* av et IT-system

- Forebyggende
- Detekterende
- Korrigerende

Sikkerhetstiltak

Fysiske

Eksempelvis:

- ✓ Låser
- ✓ Alarmer
- ✓ Vektere
- ✓ Kameraovervåkning

Tekniske

Eksempelvis:

- ✓ Kryptering/kryptografi
- ✓ Skallforsvar
- ✓ Innbruddsdeteksjon
- ✓ Tilgangskontroll
- ✓ Sikkerhets-oppdateringer (OS, firmware, software)
- ✓ Sikkerhetskopiering
- ✓ Gjenoppretting
- ✓ Redundans på tjenester

Administrative

Eksempelvis:

- ✓ Opplæring, bevissthet
- ✓ Rutiner for øvelse og hendelses-håndtering
- ✓ Sikker systemutvikling
- ✓ Definere retningslinjer, policyer, standarder
- ✓ Internkontroll og styringssystemer

I tillegg: Sikkerhetstrusler

- Trusselscenarioer: Hvem, hvorfor, hvordan?
- Sårbarheter knyttet til
  - Nettverkskommunikasjon
  - Bruk av datasystemer
  - Bruk av applikasjoner
  - Lagring av informasjon
  - Menneskelige svakheter og sosial manipulasjon
- Skadelig programvare: Typer og kjennetegn

Tastelogger

Hensikten med en *tastelogger* er å fange opp det en bruker av en datamaskin skriver på det tilhørende tastaturet. Nedenfor er det listet en rekke utsagn om tasteloggere, hvor du skal velge de du mener er korrekte.

Velg ett eller flere alternativer:

- ☑ Offentlige tilgjengelige datamaskiner, som mange har fysisk tilgang til, er ustsatt for tasteloggere.

  Ja, det vil være enkelt å installere fysiske tasteloggere.

- ☒ Bærbare datamaskiner med integrert tastatur er ikke utsatt for tasteloggere.

  Nei, laptop kan bli utsatt for tastelogger i form av skadelig programvare.

- ☒ En tastelogger er et vanlig sikkerhetstiltak som benyttes for å gjenopprette en brukers tastehistorikk i et Unix-shell.

- ☑ Fysisk sikring av datamaskiner er et egnet sikkerhetstiltak mot tasteloggere.

  Ja, kan være ett av flere tiltak.

- ☑ En tastelogger er en form for ondsinnet spionvare, som gjerne spres som en trojaner.

  Ja, en tastelogger kan både ha form som skadelig programvare og som en fysisk «dings».

Kryptering og nøkkelinfrastruktur(1)

- Nytten av kryptografi innen datasikkerhet:
  - Sikre *konfidensialitet*
  - Ivareta *integritet*
  - Bidra til *autentisitet*
  - Oppnå *uavviselighet*

Kryptering og nøkkelinfrastruktur(2)

- Kryptografiske algoritmer:
  - Hash/sjekksum
  - Symmetrisk
  - Asymmetrisk
- Nøkler, nøkkelutveksling og tilhørende utfordringer
- Hensikten med digitale sertifikater
- Digital signatur

Nytteverdi av digitale sertifikater i https

Digitale sertifikater hindrer:

- Falske nøkler og falske tjenester. Den offentlige nøkkelen til en entitet inngår i en ubrutt kjede av sertifikater (med nøkler) som går god for hverandre, helt opp til det øverste nivået, rot-sertifikatet.
- Vanskelig for svindlere å generere og spre falske nøkkelpar til allerede etablert tjeneste.

Digitale sertifikater hindrer *ikke*:

- Svindler i å opprette *et gyldig domene*, f.eks. sparebnak1.com, generere privat/offentlig nøkkelpar, og få dette signert av tiltrodd sertifikatutsteder. Fremgangsmåten benyttes ofte i svindel-angrep

HTTPS bidrar *kun* til å krypterer kommunikasjonen og verifiserer motparten.

Tillitt: Stoler dere på oss når vi ber dere gå til uio.inspera.no for å gjøre prøveeksamen? ☺ **Tips:** Sjekk sertifikatet i nettleseren.

Personopplysningsvern

Hva er en personopplysning:

- ✓ Særlig kategorier personopplysninger
- ✓ Ordinære personopplysninger

Viktig i Personvernforordningen:

- ✓ Registrertes rett til privatliv
- ✓ Lovlighet av behandlingen (hjemmel/samtykke/hvilke data)
- ✓ Åpenhet om behandlingen (til hva)
- ✓ Hvor lenge
- ✓ Krav til *informasjonssikkerhet*

Tjenesteutsetting og sky

- Tjenesteutsetting
- Skytjenester

} Gir andre tilgang til «dine» data

- Sikkerhetsmessige utfordringer knyttet til behandling av informasjon, og spesielt personopplysninger, når data behandles hos en 3.-part.

Vurdering av trussel og risiko

- Kunne anvende de hittil nevnte punktene til å gjøre en enkel *trusselmodellering* (sikkerhetsvurdering) av et gitt scenario.

- Risikoanalyse innebefatter også vurdering av potensielle *kostnader/tap*, og ender opp i en prioritering av nødvendige sikkerhetstiltak.

Trusselmodellering

For enkelhets skyld benytter en liten gruppe ansatte i en underavdeling i Forsvarsdepartementet en og samme brukeridentitet og passord for å autentisere seg i et saksbehandlingssystem.

Denne gruppen ansatte har en superbrukerrolle i saksbehendlingssystemet, som medfører utvidede privilegier sammenlignet med en ordinær ansatt i departementet. Blant annet har de privilegier til å både endre og slette *alle* lagrede dokumenter og saker.

Velg de utsagnene som er korrekte med bakgrunn i dette scenariet.

- ☒ Så lenge de ansatte har de samme privilegiene har det ingen hensikt å utstyre hver enkelt ansatt med en egen brukeridentitet.
- ☒ Det er mindre sannsynlig at passord kommer på avveie når det kun er ett felles passord å håndtere.
- ☑ Selv om de ansatte har de samme privilegiene er det nødvendig å kunne knytte hendelser til enkeltpersoner, og dermed enkeltbrukere, for å sikre sporbarhet.
- ☑ Når hendelser i saksbehandlingssystemet ikke kan knyttes til en enkeltperson kan det være vanskelig å etterprøve endringer i systemet som skyldes for eksempel menneskelige feil.

Helhetlig prosess



Innebygget personvern

Personvern skal ivaretas etter gjeldende lovverk, fra designfase til produksjon, og *i hele organisasjonens virke.*



Innebygget sikkerhet

Sikkerhet skal ivaretas fra designfase til produksjon, og *i hele organisasjonens virke.*

Kontinuerlig prosess

- Må innarbeides som en viktig del av virksomhetens prosesser
- Selges inn til en virksomhets ledelse
- Sikre datasystemer = å skape verdi
- Sikkerhet koster
- Manglende sikkerhet koster (mer?)



Kontakt:



PM eller tagg på Mattermost



Send en epost: kritisk@ifi.uio.no

Takk for i dag!

mn.uio.no/ifi

