UiO : Institutt for informatikk

Datateknologi og sikkerhet

IN1020 – Introduksjon til datateknologi

23.11.2022

Kristin Skar
kritisk@ifi.uio.no

Pensum datasikkerhet

- Utvalgte kapitler og deler av kapitler fra læreboka «Datasikkerhet».
- Stoff gjennomgått på forelesninger og i temavideoer.
- Alt av ukeoppgaver.
- Obligatorisk oppgave nr 3.
- 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 KIT (CIA)**

- **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

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 – ingen nøkkel, kun *hash-funksjon.*
  - Integritetssjekk, sammenligning av filer, beskyttelse av passord.
- Symmetrisk – *en* hemmelig nøkkel
  - Kryptering av data: Samme nøkkel for kryptering og dekryptering.
- Asymmetrisk – *nøkkelpar* av privat (hemmelig) + offentlig nøkkel
  - Kryptering av data: Offentlig nøkkel brukes for kryptering, *tilhørende* privat nøkkel brukes for dekryptering.
  - Digital signatur: Privat nøkkel brukes for signering og *tilhørende* offentlig nøkkel brukes for validering.

Kryptering og nøkkelinfrastruktur(3)

- Kjernen i asymmetrisk kryptering for sikkerhet ligger i å ha tillitt til nøklene = god *nøkkelhåndtering:*
  - Nøkkelpar, trygg oppbevaring, nøkkelutveksling og tilhørende utfordringer. Ivareta KIT.
  - Forstå hensikten med digitale sertifikater
  - PKI – Infrastruktur for bruk av asymmetrisk kryptografi (offentlig nøkkel-kryptering)

Nytteverdi av digitale sertifikater for 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.

Hvordan ivareta sikkerhetsmål? Innføre *sikkerhetstiltak*

For alle *datatilstander*

- Lagring
- Overføring
- Bruk

I ulike *faser* av et IT-system

- Forebyggende
- Detekterende
- Korrigerende (gjenopprettende)

Sikkerhetstiltak

Fysiske

- ✓ Låser
- ✓ Alarmer
- ✓ Vektere
- ✓ Kamera-overvåkning

Tekniske

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

Administrative

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

Personopplysningsvern

Hva er en personopplysning:

- ✓ Særlige 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.

- *Når data behandles hos en 3.-part:* Ansvar og sikkerhetsmessige utfordringer

Sikkerhetstrusler

- Trusselscenarioer: Hvem, hvorfor, hvordan?
  - Typiske trusler mot de ulike sikkerhetsmålene
- Skadevare: Typer og kjennetegn. Hackerens «verktøykasse».
- Vanlige sårbarheter og angrepsvektorer knyttet til
  - Nettverkskommunikasjon
  - Bruk av datasystemer
  - Bruk av applikasjoner
  - Lagring av informasjon
  - Menneskelige svakheter og sosial manipulasjon

Hva kan gå galt: 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 saksbehandlingssystemet, 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 men en egen brukeridentitet.
- ❑ Det er mindre sannsynlig at passord kommer på avveie når det kun er ette 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 knytte 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?)

UiO : Institutt for informatikk

Takk for i dag!

mn.uio.no/ifi