

UiO : Institutt for informatikk

Å innfri sikkerhetsmål

Autorisert og uautorisert tilgang

IN1020 – Introduksjon til datateknologi
Forelesning 21.08.2026

Kristin Skar
kritisk@ifi.uio.no

Datateknologi og sikkerhet

Tema for tema:

1. Datasikkerhet - Er det så viktig da? (19. aug)
2. **Å innfri sikkerhetsmål: Autorisert og uautorisert tilgang (21. aug)**
3. Hvordan hackes vi? Trusselaktører og angrepsvektorer (26. aug)
4. Kryptografi – nøkkelen til (fungerende) digital samhandling (9.sept)
5. Trygg infrastruktur og sikre datasystemer (18.sept)
6. Å skape trygge digitale tjenester krever innsats (23.sept)

Å innfri sikkerhetsmål: Autorisert og uautorisert tilgang

Ressurser:

- Forelesning 21.08.26
- Ukeoppgaver og pensumlitteratur:
  - Jøsang: Kap 1, Kap 8 (s.185-196 + 8.5.1, 8.5.4, 8.6), Kap 10 (10.1, 10.2, 10.5, 10.7.1)
  - 2 artikler fra Datatilsynet

Nøkkelord:

- Sikkerhetsmål
- Autentisering
- Tilgangsautorisasjon og tilgangskontroll

Sikkerhetsmålsetninger

KIT

- Konfidensialitet
- Integritet
  - Dataintegritet
  - Systemintegritet
- Tilgjengelighet
- Personvern
- Autentisitet
  - Brukerautentisitet
  - Systemautentisitet
  - Dataautentisitet
- Ubenektelighet
- Sporbarhet

Personopplysningsvern



Rett til privatliv?

Rett til innsyn?



Rett til å bli glemt?



Lovverk stiller strenge krav til behandling av personopplysninger.

Prinsipper for behandling av personopplysninger

Personopplysningsloven (GDPR) artikkel 5:

- Lovlighet, rettferdighet og åpenhet
- Formålsbegrensning
- Dataminimering
- Riktighet
- Lagringsbegrensning
- Integritet og konfidensialitet

Lovtekst: https://lovdata.no/lov/2018-06-15-38/gdpr/a5

Refleksjon

Du er innlagt på sykehus for en operasjon.
Hva er viktigst for deg som pasient:

- Konfidensialitet
- Integritet
- Tilgjengelighet

Helse Sør-Øst: Innrømmer at utenlandske IT-arbeidere fikk tilgang til sensitiv pasientdata.

De siste ukene har titalls IT-arbeidere i Asia og Øst-Europa hatt tilgang og utvidete rettigheter til datasystemet til Helse Sør-Øst, viser informasjon NRK har innhentet. De har hatt mulighet til å hente ut pasientdata til 2,8 millioner nordmenn.

«De norske IT-arbeiderne i helseforetaket har underskrevet taushetserklæringer. Nasjonal sikkerhetsmyndighet har gitt NRK informasjon om at det ikke er mulig å sikkerhetsklarere folk fra Bulgaria, Malaysia og India. Det er fra disse landene driften av IT i Helse Sør-Øst etter hvert skal foregå.»

Kilde: nrk.no

«Et stort antall IT-arbeiderne fra Asia og Øst-Europa har siden medio mars kunnet gå inn og kopiere pasientjournaler til 2,8 millioner nordmenn uten å legge igjen spor.»



Måtte avbryte undersøkelse på Sykehuset Østfold på grunn av PC-oppdatering

Pasienten ble liggende i unødvendig narkose i én time.

Kilde: dagsavisen.no

Hackere lammer datasystemer på sykehus

Sykehus og myndigheter i mange land ble fredag utsatt for et omfattende dataangrep. Hackerne angriper via e-post og krever løsepenger for å åpne maskinene igjen.

Dr. Tarek Seda på King's Mill Hospital sier til BBC at det er kaotiske forhold på sykehuset, og at arbeidet tar enormt lang tid fordi alt må gjøres manuelt. Sykehuset har måttet utsette viktige operasjoner. Dr. Seda kaller angriperne feige.



Kilde: nrk.no

Sykepleier anmeldt for snoking i journal:

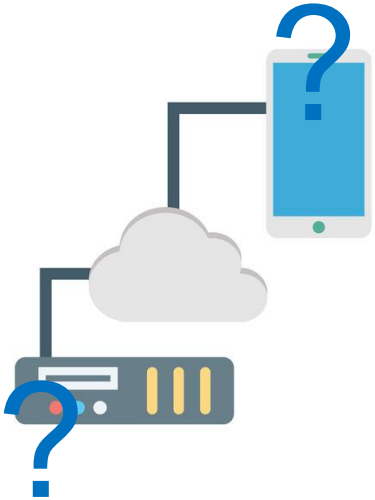
En sykepleier ved Sykehuset Levanger er anmeldt for å ha snoket i journalen til en kollega. Nå beklager sykehusdirektøren, skriver Trønder-Avisa. (….) Kvinnen oppdaget snokingen da hun begjærte innsyn i loggen til sin egen journal. Der kom det fram at en sykepleier hadde gått gjennom samtlige journalnotater siden 2004.

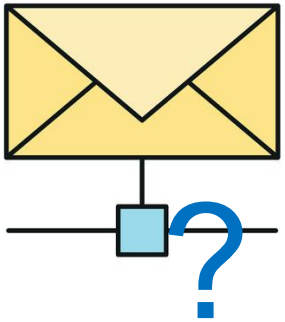
Kilde: dagbladet.no

- Brudd på hva (KIT)?
- Hvem utgjør trusselen?
- Hvordan oppdages angrepet?

Problemstilling: Hvem er hvem på internett? Og stemmer det?







Skatteetaten

Entiteter og identiteter

- Entitet?
  - Noe som har fysisk, juridisk eller prosessuell eksistens
  - Entiteter kan gis en *identitet*, som gjør det mulig å referere til entiteten
- Identitet?
  - Representasjon av entiteten, gjennom et sett med attributter som er tilordnet entiteten
  - *Kan kjenne igjen entiteter basert på identiteten*
  - Som regel har man *identifikator*
- Digital identitet?
  - Digital representasjon av en *entitet*, gjennom bruk av digitale, maskinlesbare data (*attributter*)
- Identitetshåndtering er *prosessen med å registrere og autentisere identiteter*

Autentisitet

- Hvordan muliggjøre tillitt til at *identiteter (entiteter)* er autentiske:
  - Autentisk *individ (bruker, person)*?
  - Autentisk (data-)*system*?

- I tillegg ønske om
  - Autentisk *opprinnelsen til data* (ofte kalt *en melding*)?

Autentisering

- Autentisering er mekanismen for å bekrefte en hevdet identitet:
  - *brukerautentisering*
  - *systemautentisering*
  - *dataautentisering*

Brukerautentisering

Å verifiserer en hevdet identitet for en bruker.

- Hvordan oppnå *brukerautentisitet* (også kalt *personautentisitet*)?
  Svar: Bruk av *autentiseringsfaktorer*



Brukerautentisering

Autentiseringsfaktor

- Tre hovedkategorier *bevismateriale* (autentiseringsfaktor) for identitet: Noe du vet, noe du har og/eller noe du er
- Kombinasjon av flere faktorer er vanlig

"Always remember the three main authentication factors: What can be easily guessed, what can be left in a cab, and what can be chopped off"

Autentiseringsfaktor: Noe du vet

Eksempler:

- Passord til IT-system
- Kode til elektronisk dørlås
- Mønster du husker

Fordel?

- Du har det alltid med deg

Ulempe?

- Lett å glemme
- Lett å gjette for uvedkommende
- Lagres på datamaskin? Nedskrevet?
- Lagres hos tjenesteleverandør
- Ikke veldig sikkert

Koder/passord kan knekkes

- Passord lagres som hovedregel ikke i klartekst
- Likevel kan de «knekkes»:
  - Systematisk gjetting *(brute-force)* og «ordlisteangrep»
  - Utnytte svakheter i datasystemene
  - Intelligent søk. Kunnskap om deg?

- https://haveibeenpwned.com/

123456	1234567	abc123
password	football	starwars
12345678	iloveyou	123123
qwerty	Admin	dragon
12345	monkey	passw0rd
123456789	welcome	Master
letmein	login	superman

Autentiseringsfaktor: Noe du har

Eksempler:

- Nøkkel til lås
- Engangspassord fra *kodegenerator*
- Sekundære kanaler
- Kontaktløse brikker (RFID-kort)
- Enhet med lagrede *passnøkler*

Fordel?

- Du slipper å huske

Ulempe?

- Lett å miste
- Kan stjeles/«lånes»
- Glemmes hjemme?

Autentiseringsfaktor: Noe du er - *biometri*

Eksempler:

- Ansiktsgjenkjenning
- Fingeravtrykk
- Scanning av øyet
- Signatur
- Ganglag

Fordel?

- Du slipper å huske
- Du har det alltid med deg

Ulempe?

- Unikt nok?
- Permanent nok?
- Sikkert nok?
- Krever ekstrautstyr (sensorer, lesere, ol)
- Ressurskrevende å sammenligne

Flerfaktor-autentisering

Utfordring: Passord kan gjettes, objekter kan mistes/stjeles

Løsning: Autentisering med kombinasjon av flere faktorer

- Kombinasjon av to eller flere ulike faktorer
- Øker sikkerheten betydelig, men autentisering blir mer tungvint for den som skal autentisere seg.
- Økende antall tjenester tilbyr flerfaktor- eller tofaktor-autentisering (2FA)

Autentiseringsløsning som tjeneste

Aktører tilbyr elektronisk identitet og autentisering som en tjeneste.

- **Eksempler**: Google, Facebook, autentiseringstjenester for e-forvaltning (Feide, BankID, mfl.)
- **Fordeler**?
  - God kompetanse, ekspertise og dermed økt sikkerhet i tjenesten som tilbys
  - Brukerne må forholde seg til færre brukeridentiteter/passord
- **Ulemper**?
  - Knekkes autentiseringsfaktoren(e) vil hackere ha tilgang til flere tjenester som deg.
  - Vane å logge inn gjør oss til et enkelt mål for svindel.

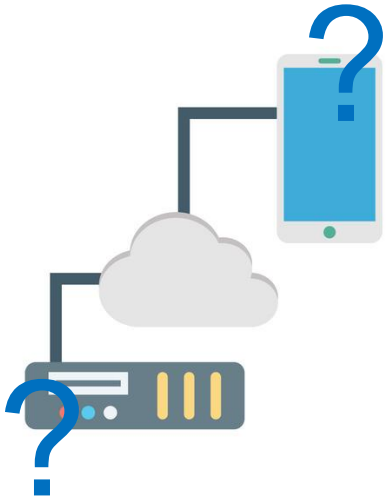
Autentiseringsnivå

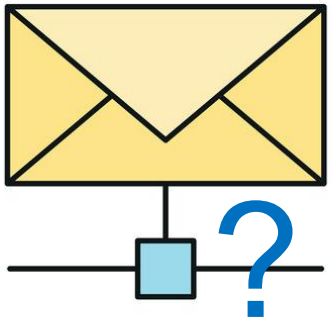
- *Autentiseringsnivået* bestemmes av den kombinerte *styrken* til alle faktorene som benyttes i en autentiseringsordning.

- «E-postkontoen er navet i ditt digitale liv»

Autentisering av systemer og data?







Systemautentisering

Å verifisere at et *system* er ekte, altså det det utgir seg for å være, i en online interaksjon.

- Hvordan oppnås *systemautentisitet*?
  Svar: Bruk av *kryptografi*



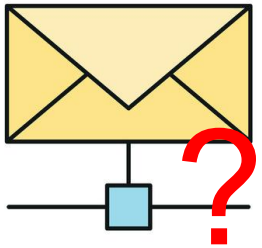
Skatteetaten



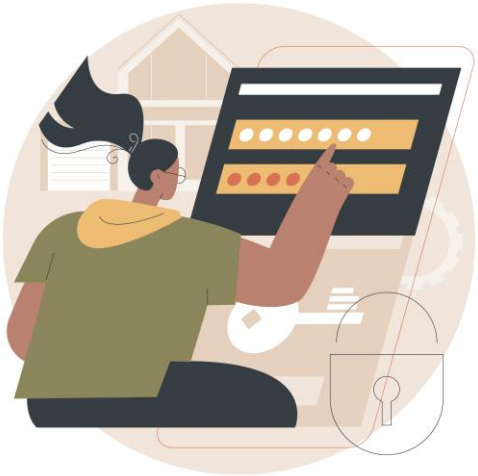
Autentisering av dataopprinnelse

Å verifisere opphav til/avsender av data/melding.

- Hvordan oppnå *dataautentisitet*?
  Svar: Bruk av *kryptografi*



Tilgang?



- Nødvendig å kunne styre *tilgang* til *ressurser*.
- Hvem *beslutter* hvem som skal ha tilgang til hva?

Tilgangskontroll

Tilgangskontroll er sikkerhetsmekanismen som bidrar til at bruker/enheter kun får tilgang til ressurser de er skal ha tilgang til:

Tilgangskontroll = autentisering + autorisasjon

Tilgangsautorisering

«Å autorisere er å godkjenne eller gi løyve»

snl.no

- Tilgangsautorisering er å *spesifisere* tilgangsrettigheter for brukere/enheter.
- Tilgangsautorisering er altså **ikke** teknologi, men policy.
- Eksempel på en slik policy:
  «En ansatt i lønnsavdelingen skal ha tilgang til lønnssystemet.»

Tilgangskontroll

Tilgangskontroll benytter seg av forhånds-spesifiserte tilgangsrettigheter for å beslutte om tilgang til ressurser skal gis eller ikke når en autentisert bruker/enhet gjør en forespørsel om tilgang.

Eksempler på forespørsler fra *subjekter* for *objekter*:

- Alice vil lese innholdet i en fil
- Bob vil oppdatere kontobalansen på en bankkonto
- Kirurgen vil oppdatere en pasientjournal etter operasjon
- En applikasjon vil opprette en nettverksforbindelse mot en annen maskin

Hvem styrer tilgang?

Alle datasystemer må ha en funksjon som har som oppgave å håndtere forespørsler om tilgang fra subjekter for objekter:

1. Kontrollere forespørsel mot gjeldende policy
2. Innvilge eller avvise tilgang
3. Logge hendelsen til hendelseslogg (ivaretar sporbarhet)



Refleksjon:

Betyr det at du *har tilgang til en ressurs* at du også er *autorisert* til ressursen?

Tilgang, logging og sporbarhet

- ✓ *Loggføring* av hendelser er bidrag til sikkerhetsmålet *sporbarhet*.
- ✓ Kan loggføring av hendelser ha flere funksjoner?
- ✓ Kan vi stole på hendelsesloggene?
- ✓ Hvor lenge kan logger lagres?





Refleksjon:

Har all informasjon samme beskyttelsesbehov?

Læringsmål for økten

- Forstå sikkerhetsmålet *autentisitet*, kjenne til de ulike formene for *autentisering*, samt styrker og svakheter ved ulike *autentiseringsfaktorer.*
- Ha god forståelse for begrepet *tilgangsautorisering*
- *Tilgangskontroll*: Vite hva som er de nødvendige elementene i tilgangskontroll, vite hvordan tilgangskontroll fungerer, og hva som oppnås.

Takk for i dag!

mn.uio.no/ifi

