IN1020 uke 6

GRUPPE 10

Plan for dagen

- Datasikkerhet
- Sikkerhetsmål
- Sikkerhetstiltak
- Autentisering
- Tilgangskontroll
- Lab

Datasikkerhet

- Mer teoretisk, sammenlignet med programmeringsdelen

- Utrolig relevant:
  - Finnes eget fag for det (IN2120 – Informasjonssikkerhet), (Master i informasjonssikkerhet)
  - Mange andre emner som omhandler sikkerhet

- Finnes mange betegnelser som **omtrent** handler om det samme:
  - Informasjonssikkerhet
  - Digital sikkerhet
  - Cyber sikkerhet
  - IT sikkerhet

Datasikkerhet

- Sikkerhet: Defineres som en **tilstand** der man føler seg fri fra fare og frykt og uønskede hendelser

- Handler om å beskytte en **verdi**:

- Verdi: Noe som er viktig for deg:
  - Abstrakt: Informasjon
  - Konkret: Gjenstander

Kule lenker

https://haveibeenpwned.com/

https://www.proxynova.com/tools/comb/

http://lastbit.com/pswcalc.asp

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD

HIVE SYSTEMS

-Data sourced from HowSecureismyPassword.net

Sikkerhetsmål

- Et sikkerhetsmål er en egenskap man kan ønske å oppnå eller tilby.
- Sikkerhetsmål:
  - **Konfidensialitet**
  - **Integritet**
  - **Tilgjengelighet**
  - Autentisitet
  - Uavviselighet
  - Sporbarhet
  - Personvern

Sikkerhetsmål: *CIA* (KIT på norsk)

- **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.

Sikkerhetsmål: 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**

Sikkerhetsmål: 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.

Sikkerhetsmål: 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.

Sikkerhetsmål: Personvern



Rett til privatliv?

Rett til innsyn?



Rett til å bli glemt?



Lovverk stiller strenge krav til behandling av personopplysninger.

Behandling av personopplysninger

Personopplysninger er alle opplysninger og vurderinger som er mulig å knytte til deg som enkeltperson.

Skiller mellom:

Alminnelige personopplysninger

- Navn, brukernavn, telefonnummer, studentnummer, adresse, IP-adresse, fingeravtrykk, adferdsmønster, mm.
- Fødselsnummer? Kun ved saklig behov.

Særlige kategorier personopplysninger

- Helseopplysninger, seksuell legning, religion, straffedommer, etnisk opprinnelse, fagforeningsmedlemskap, mm.

Sikkerhetstiltak

- Et sikkerhetstiltak er noe som gjøres for å oppnå/ivareta sikkerhetsmål.
- Sikkerhetstiltak er basert på *spesifikk implementering*.
- Sikkerhetstiltak kan brukes for å *forebygge*, å *oppdage*, eller å *gjenopprette*

Sikkerhetstiltak kan kategoriseres

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*

Sikkerhetstiltak for ulike *tilstander*

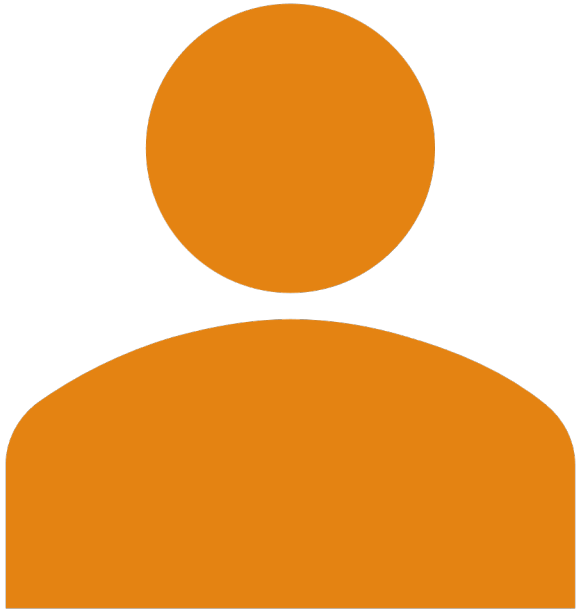
- Informasjon kan befinne seg i ulike tilstander:
  - Når den *lagres*
  - Under *overføring*
  - Når den *er i bruk*
- Ulike tilstander krever ulike sikkerhetstiltak.

➢ Informasjon må beskyttes i enhver mulig tilstand informasjonen kan befinne seg i.

Sikkerhetstiltak i ulike *tidsfaser*

- *Forebyggende* (preventive) tiltak:
  - Forhindre og avskrekke angrepsforsøk.
- *Detekterende* (avdekkende) tiltak:
  - Varsle angrep som forsøkes eller som allerede er skjedd.
- *Korrigerende* tiltak:
  - Gjenopprette skade på informasjonsressurser etter angrep.

➢ Det er alltid nødvendig å benytte en kombinasjon av tiltak fra alle tre faser for å opprettholde dekkende beskyttelse.



Autentisering

Å BEKREFTE EN HEVDET IDENTITET

Autentiseringsfaktor

- Noe du vet:
  - Er noe som ligger i minnet på mennesker
  - F.eks. passord, kode
- Noe du har:
  - Er en du eier, fysisk artefakt
  - F.eks. kodebrikke, bankID på mobil, RFID-kort, studentkort
- Noe du er:
  - Menneskelig egenskap eller trekk, biologisk mennesketrekk
  - F.eks. fingeravtrykk, FaceID, Scanning av øye, stemmegjenkjenning
- Flerfaktor-autentisering -> bedre sikkerhet

Ulike autentiserings typer

- Brukerautentisering:
  - Verifisere hevdet identitet
  - Oppnås ved bruk av autentiseringsfaktorer
- Organisasjonautentisering:
  - Verifisere at organisasjon/virksomhet er ekte, altså den den utgir seg for å være
  - Kan oppnås ved bruk av kryptering
- Systemautentisering:
  - Verifisere at et datasystem er det det utgir seg for å være
  - Oppnås ved bruk av kryptering
- Autentisering av dataopprinnelse
  - Verifisere at meldingen/data man mottar kommer fra en hevdet sender OG at innholdet ikke er endret underveis i forsendelsen
  - Oppnås ved bruk kryptering

Scenario

- Du drar på ifi en lørdagskveld for å øve til eksamen i IN1020
- Du skanner studentkortet ditt og taster inn et 4 sifret kode
- Hvilke autentisering faktor blir oppfylt?



Autorisering



Handler om å avgjøre om en bruker skal ha tilgang til informasjon eller tjeneste



Å autorisere er å spesifisere en tilgangs-policy



Autorisering er altså **IKKE** teknologi, men policy



Eksempel på en policy som jeg **FANT PÅ**:

«Gruppelærere skal ha tilgang til studenters obliger for å rette dem»

Tilgangskontroll

- Tilgangskontroll = Autentisering + autorisasjon
  - 1. Sjekk om identiteten er det den utgir seg for å være
  - 2. Sjekke om identiteten skal ha tilgang etter reglene/policy manifestert i autorisasjon
- Autorisasjon er altså å definere policy for tilgang
- Mens tilgangskontroll er å håndheve eller overholde policyen i et datasystem

Lab

- Jobbe videre med oblig eller ukesoppgaver
- Send meg mail eller teamsmelding hvis dere lurer på noe eller trenger hjelp til oblig
- myhd@uio.no