# Forelæsningsnoter

Mikkel Boye Rasmussen

06.02.2023

# Introduktion til Informationssikkerhed

### Lidt om netværk

*WLAN - implementeret med WiFi*
*LAN - implementeret med ethernet kabel*

### Top 6 cyberhacks fra sidst

### Ransomware - den nye vinder

- target bliver inficeret med software der krypterer hele deres system.
- der kræves løsesum for at åbne systemet igen
- den inficerede software bliver placeret via en sårbarhed.
- I starten mange små ofre, i dag er der mange store virksomheder der bliver ramt.
- Trend: targets er oftere og oftere kritisk infrastruktur/forsyning.

*eksempel må ransomware - krypteret brugerens system countdown til slettelse af filer*

Ransomware eksempler i Danmark

- Mærsk
- Demant
- Kalundborg forsyning
- Europæiske Hospitaler, incl. Danmark

Et godt ransomware angreb beslaglægger også backuppen - lokale backups laves måske på ugentlig basis - hvor meget data kan man tåle at miste?

*Business continuity plan - RPO, RCO: hvor meget data kan vi miste, hvor hurtige skal vi være?*

*Incident response plan - hvordan reagerer man ved angreb?*

**Case: Kalundborg forsyning ramt af ransomware**
Gik med det samme igang, kan ikke sige meget om omfanget. Ved intet om hvordan virus kom ind. Opfordrede kunder til at være ekstra opmærksomme i den nærme periode.

*Persondata PII - Personal Identifiable Information (den rigtige betegnelse for hvad vi kalder persondata i Danmark)*

Da kalundborg forsyning er kritisk infrastuktur er der direkte samarbejde med politi og center for cybersikkerhed.

*offentlige institutioner - kan maks få en bøde på 2mil euro.*

*private virksomheder - 2% af global omsætning.*

*center for cybersikkerhed skal underrettes indenfor 72 timer, efter NIS2 opsættes et 24-timers krav også.*

**Grundlæggende strukturer**

1. trusler
2. sårbarheder
3. risikoanalyse
4. tekniske og orginisatoriske foranstaltninger
5. rest-risiko

**3 kategorier - samt typiske brud**

- fortrolighed (confidentiality) - Læk af sensitiv data.
- integritet (integrity) - Manipulering af data.
- tilgængelighed (availability) - eksempelvis DDoS

*Ovenstående 3 forkortes CIA.*
*Der skal være tale af en af ovenstående 3 for at snakke om brud på IT-sikkerhed*

**Fortrolighed**

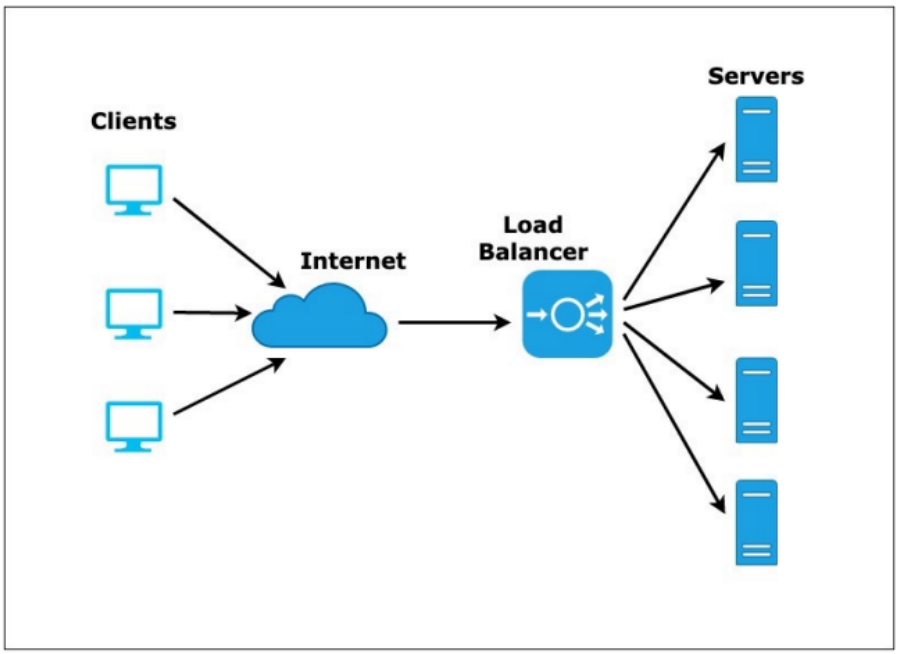
- Kryptering/Hashing (hashing er irreversibel kryptering)
- Adgangsstyring
- funktionsadskillelse

**Fortrolighed**

- Logning - se hvem har gjort hvad?
- Change management - visualiser ændringer
- Test - test for korrekt data
- Feldtkontrol - kontrollering af inputfelter, eksempelvis @ i email
- Awareness

**Tilgængelighed**

- Backup
- Redundans
- Serviceaftaler
- Loadbalancing
- Patching



**Big Scams**

- Norfund - mistet 10million usd fra email scam
- iss - malware lukkede virksomhedens systemer i 18 dage, mistede 20% af virksomhedens værdi.
- Mærsk - mistede en millard kroner - stort hackerangreb fra Rusland, virus kaldet NotPetya som satte computere og software ud af drift.

**Incident Event Cycle** Incident cycle with meassures

- Incident cycle with meassures
- Threat (Reductive)
- Preventive
- Incident (Detective)
- Repressive
- Damage
- Recovery
- Corrective
- Evaluative

Alternativt (og på dansk)

- Begrænsning
- Forhindring
- Opdagelse
- Undertrykkelse
- Korrigering.

**Foranstaltninger (meassures)**

Categories

- reductive
- preventive

- detective
- responsive recovery/corrective
- evaluation

Typer

- Organisational/procedural/administrative
- physical
- technical/logical

# Netværk

Addressering

*Analogi: Brev vs Router*

**TCP og UDP**

three-way-handshake
netværkspakke - indeholder checksum og request-header

# Præsentation fra HK

IT-security from a software developer's perspective
Om kristian (Forelæseren)

- partner i app academy
- former IT consultant
- klh@appacademy.dk

**Første historie: Mat Honan**
Hackede twitterprofil da han havde handlet @mat, hvilket havde lidt status. Hans mailadresse var offentligt tilgængeligt mange steder grundet hans job. Apple tillod oplåsning af emailkonti hvis man oplyste billing address, amazon konto og 4 sidste kortoplysninger. - de slog domænenavnet op og tog de tilknyttede adresse - de ringede til amazon og sagde de havde fået nyt dankort - ændrede mailadresse på amazon da de kunne oplyse dankortoplysninger - de kunne se nye og gamle kreditkort - de første tal er XXXX og de sidste var fremvist. - nu har de alle oplysninger til nulstilling af email, og kunne tage

hans twitter. - hackerne slettede alt for at stresse Mat, således de havde mere tid til at hacke twitterkontoen.

**Some good things to do**
two-factor authentication
pas på hvad man opbevarer af data, eksempelvis kreditoplysninger

**MitID** er two factor sikker?

**hvordan bliver gmail konti typisk hacket**
brug af samme kodeord andre steder, ved databrud er de frit tilgængeligt.

**a challenge**
As a software developer, i want to save user details, how to
hashing + salting

hvorfor er hashing ikke tilstrækkeligt?
rainbow tables.

the problem with all solutions- the more code, the more possible security holes.

**Phishing af 2FA Tokens** se videoen vedlagt på moodle

**how twitter was attacked** eksekverbar javascript kode i tweets Cross-site scripting

**how BCGE was blackmailed - banque cantonale de genéve** beslaglagt kundedata, hvis ikke betalt ransom, slettes kundedata. banken fandt ud af data indeholdte både kunder og ikke kunder så noget var off. det var kun deres kundeformular og ikke deres, reelle bankdetaljer.

**Supply chain attack** Kode bygges ikke fra bunden, men bygges på pakker. Pas på med brugen af pakker.
*itegrity param på script tags for at modvirke JS injections.*

**The first known cyber weapon**
Stuxnet - plutoniumberigning, ødelæggelse af centrifuger via hacking. de computere tilknyttet berigningen har været i en lukket bobbel som ikke gik på nettet. kiggede efter et specifikt siemens system på computeren, ellers gjorde den intet. inficerede usb-nøgler der blev indsat i de inficerede devices, dette smittede diverse devices. virussen manipulerede centrifugernes hastighed, samt fremviste data fra en time siden for ikke at blive opdaget.

**Yderligere cases:**
Solarwinds - hacking af system-management tool.
Maersk - utilsigtet krypteret af hele deres system.
Viasat - sattelitter i ukraine blev hacket.