Vi ruler!! <3 GOOO TEAM

Sikkerhet og robusthet i IKT systemer - Kompendium

Komplekse systemer:

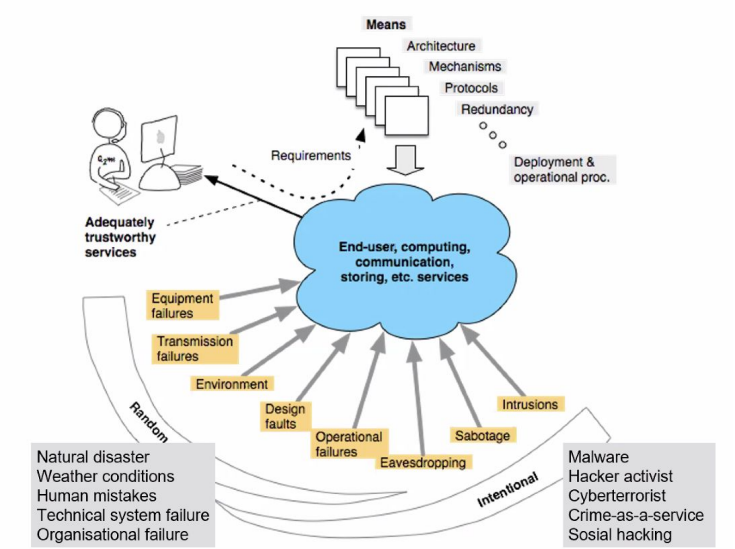
- Kommunikasjonsteknologi - er muliggjørende teknologi som samfunnet behøver (logistikk, transport, helsetjenester..) men må være sikkert og robust for at de tjenestene skal fungere optimalt.
- IKT infrastruktur - Service, informasjon infrastruktur og fysisk infrastruktur (networks, computing and storage facilities). Den fysiske infrastrukturen endres ikke like ofte som tjenester og informasjon.

Trusler:

- Er ikke offentlig kunnskap hvordan nett er bygd med tanke på trusler.
- Eks, online banking. Brukere må vite at de er koblet til den faktiske banken. informasjon må holdes hemmelig.
- Type trussel, man in the middle angrep, noen router infor annerledes, og endrer informasjon som sendes fram og tilbake

Det brede spekteret av trusler som kan skje:

Random - ting som skjer uten ond hensikt
Intentional - noen med onde hensikter angriper med itensjon. Her man ser på sikkerhet



ital sårbarhet – sikkert samfunn Beskytte enkeltmennesker og samfunn i en digitalisert en" (NOU 2015:3)

Mange aktører involvert:

- Vi har et nettverk av nettverk
- spenner over hele verden
- har ISPer som tilbyr nettverk
- for å ha tjenester oppe må disse samarbeide
- må derfor ha standardiserte nettverksprotokoller
- alle aktørene stoler ikke på hverandre og er konkurrenter

ICT trender

Fysisk infrastruktur

- Fysisk mindre
- større kapasitet
- mer embedded (en del av)
- billigere

Vi ruler!! <3 GOOO TEAM

Services/tjenester
- mer avansert funksjonalitet
- mer allsidig
- allstedsnærværende

Informasjon
- big data
- AI
- Regulering(GDPR)

Struktur
- mer connected
- økt dynamikk
- økt kompleksitet
- autonomi

Trendene påvirker risikoen. Eks, økt kompleksistet. da øker sannsynligheten for at noe går galt. Færre personer som forstår seg på kompleksiteten og store konsekvenser når det går galt.

7 eksempler på kritisk infrastruktur:
Bank og finans, petroleum, transport, energi, kommunikasjon og informasjonsteknologi, gass og vann og vannsystemer.

Ekomnettet:

Ekom - elektronisk kommunikasjon
Ekomtjenester er tele, internett og taletjenester

Konsekvensene om Ekom går ned er store for bla liv og helse, økonomi og samfunns stabilitet. Det viser hvor avhengig samfunnet vårt er av IKT.

DEL 2 Kategorier av sikkerhet og robusthet - Taxonomi

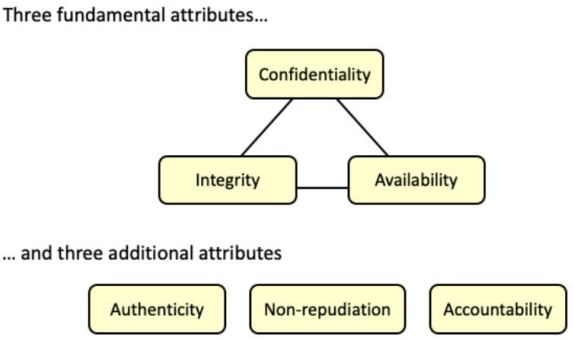
Sikkerhet, robusthet og pålitelighet - sier noe om kvaliteten og egenskapene til en tjeneste

"Needto know" means that only those who need the information should gain access to it but sometimes lack of i nformation can cause even bigger harm ("need-to-share").

Vi ruler!! <3 GOOO TEAM

5 kategorier av sikkerhet og robusthet:

- **Security** - Data Security, Information Security, ICT security, Cyber security
- **Dependability**
- **Privacy**
- **Performance**
- **Safety**



Security - sikkerhet:
Confidentiality: Handler om informasjon. Kun de som skal ha tilgang, har tilgang. For eksempel skal færrest mulig ha tilgang til sensitiv informasjon. Å sikre seg om at informasjon bare er lesbar for de som faktisk skal lese den.

Integrity: Handler om informasjon og systemer som prosesserer det (må være riktig og komplette). Du kan stole på at de opplysningene du ser stemmer.
For å ha integritet trenger vi non-repudiation og authenticity.

Availability: Fokus på informasjon og informasjonssystemer. Data skal være tilgjengelig for de som har lov til å bruke dem.

<u>Tilleggsattributter</u>
Authenticity: Handler om å garantere gyldighet av for eksempel en melding. Verifisere kilden av informasjonen. Ofte senderen.

Non-repudiation: Handler om å ikke kunne nekte at man har sendt eller mottatt informasjon over nettet etterpå. Kan også handle om å ikke nekte en digital handling som å slette en fil.

Accountability: Handler om at hvis andre attributter feiler. Er ikke mulig å lage sikkert system så man må kunne spore feilene i etterkant.

Security vs usability

- Viktig at sikkerhet er brukbar så det fungerer som det skal. Kan ikke sette sikkerhet så det ikke blir brukt
- Eksempel - email sikkerhet. Ingen god løsning ende til ende. Det er vanlig at det blir kryptert fra server til server, men ikke på vei til server

Dependability - Pålitelighet:
Skal kunne stole på at systemet leverer tjenesten den har lovet.

Availability: Fokus på service. Systemet skal være tilgjengelig for de som skal bruke det på et gitt tidspunkt.

Availability	Downtime per Year
One nine (90%)	36.5 days
Two nines (99%)	3.65 days
Three nines (99.9%)	8.76 hours
Four nines (99.99%)	52.56 minutes
Five nines (99.999%)	5.26 minutes

Vi ruler!! <3 GOOO TEAM

Kan måle tilgjengelighet - se bildet til høyre.
Asymptotisk tilgjengelighet - hva er sannsynligheten for at systemet virker på et tilfeldig tidspunkt i fremtiden. Antar at systemet har nådd sin “steady state”. Mest vanlige måten å måle tilgjengelighet. Typisk en verdi mellom 0.9 (pc hjemme uten støtte) og 0.99999 (nettverks komponent med høy availability)
Instantaneous tilgjengelighet - sannsynlighet ved et gitt tidspunkt
Interval availability - gjennomsnitt. Over perioder.

Reliability: Kontinuitet. Man skal kunne fortsette å bruke tjenesten når en har startet. Time to first failure, Time to fail.

Et system med høy availability kan fortsatt ha mange korte interrupts og derfor lav reliability. Reliability er derfor viktigere enn availability når en service som tar lenger tid ikke kan bli interrupted. Som når man skal laste ned en stor fil eller utføre tunge beregninger eller simuleringer.

Maintainability: Hvor fort man kan få opp systemet etter en fail. F eks når strømmen går. Må reparere systemet. Vil effektivisere “reparasjonstiden”.

De to tilstandene i pålitelighet - Up og down. Pålitelighet handler om å beskrive hvordan et system oppfører seg. Enten så klarer det å levere tjenesten, eller så gjør det ikke det.

Privacy:
Data som kan identifisere et individ. Handler om personopplysninger og å beskytte disse.
Terminologi:
- Personal data: Informasjonen til en person.
- Data subject: Den aktuelle personen.
- Data controller: Er enheten som bestemmer middel og formål med det personlige.
- Data processor: Et middel som kollekter eller bruker personlig data, på vegne av data controlleren.

Privacy paradox - Selv om brukere oppgir at de er interessert i personvern og klar over mulige personvernrisiko, prioriterer de nesten alltid funksjonalitet over privacy.

Seven key principles - de grunnleggende prinsippene: Lawfulness, purpose limitation, data minimization, accuracy, storage limitation, security, accountability.

Privacy vs security
Privacy is concerned with,protecting the personal data of individuals. Security is concerned with protecting any d ata or information (or of course any other asset in the ICT infrastructure, such as services and physical compone nts)

Vi ruler!! <3 GOOO TEAM

Confidentiality vs privacy:
Privacy is concerned with protecting the personal data of individuals while confidentiality is concerned with protecting any type of information from unauthorised access.

Performance - Ytelse:
Evnen et system har til å tilby tjenesten. Avhenger av mengden ressurser i systemet og utnyttelsen av dem.

Viktige attributter
Kapasitet: Maksimal belastning et system kan håndtere per tidsenhet. Kapasitet er en egenskap for et system og ikke tjenesten den leverer.
Forsinkelse: Tiden det tar å fullføre en tjeneste. End - to- end.
Throughput: mengden

Pålitelighet vs ytelse
Finnes en mellomting i motsetning til pålitelighet. Er tilgjengelig selv om det går skikkelig tregt.

Dependability og performance er ikke uavhengige properier. Et system med lav performace kan oppfattes som unavailable fra en brukers perspektiv.

Safety:
Mennesker, miljø, bygninger osv skal ikke skades.
Evnen til et system til å sørge for å levere en tjeneste uten at det skjer katastrofale feil.
IKT systemer skal være designet på en måte som ikke skader oss fysisk.
Skal ikke ha uheldig påvirkning på omgivelsene.

Safety vs security

- Safety: protection against unintended incidents. Ulykker og uhell
- Security: protection against deliberate incidents. Angrep. Med hensikt
- Trenger begge for at noe skal være sikkert
- Safe = safety + security.

De som jobber med safety er nøye med at systemet ikke kan gjøre skade på omgivelsene. Ser også på IKT systemer, men hvilke konsekvenser som at folk og bygninger kan bli skadet. Derfor viktig i maritim transport der man har verdier, og mennesker og dyr som skal passes på.
Oftest ganske uvanlig å ta med angrep når man jobber med safety. Ser på tilfeldige hendelser. Selv om angrep også kan få katastrofale konsekvenser. Det har begynt å endre seg til siste årene.

Vi ruler!! <3 GOOO TEAM

Functional vs non-functional requirements

- Funksjonelle - noe et system bør gjøre.
- Ikke-funksjonelle - hvordan et system bør oppføre seg.

Hvorfor er det viktig å identifisere ikke-funksjonelle krav(security, safety…) i en tidlig fase av systemutviklingsprosessen?
Fixing things afterwards is almost always more difficult and will lead to more complicated and costly solutions."

Assets - Verdier:

Noe verdifullt som må beskyttes. For å identifisere verdien må man se på hva som er viktig for organisasjonen eller for deg selv. Kan for eksempel være verdifullt å beskytte en database på grunn av verdifull informasjon for organisasjonen, eller kan være en tjeneste som er viktig at er tilgjengelig.

Deler i primære og sekundære verdier (primary and supporting):

- *Primary* - ofte informasjon eller tjenester for å beskytte informasjon. For en bedrift har ikke en ruter en verdi i seg selv men det har nettverket som tjenesten den leverer.
- *Supporting* - må beskyttes så man ikke kan skade primære verdier gjennom den.

Eksempel-Skype: For brukeren er det viktig at taletjenesten fungerer som det skal fordi det er det brukeren bruker Skype til. Samtidig er det viktig at chat meldinger kommer fram og ikke endres på veien. For Microsoft er en verdi tjenesten som setter opp samtaler, servere og databaser.

Typer assets: Informasjon, tjenester, software, hardware, nettverk, database, kunnskap.

Sikkerhetskrav:

Eksempel-Skype: “It must not be possible to wiretap calls” (confidentiality), “It must not be possible to alter a transmitted message”(integrity).

- Kan være vanskelig å stille gode krav.
- Typisk konflikt, need to know vs need to share: Om vi låser inn informasjon fysisk eller krypterer den får vi god konfidensialitet, men det får da utover tilgjengeligheten.
- For sterke krav til konfidensialitet gjør det vanskelig med tilgjengelighet.
- Må ha relevante krav

Vi ruler!! <3 GOOO TEAM

DEL 3 Trusler og sårbarheter

Sårbarheter, trusler og failure

Historisk - amerikansker forsvaret med det første nettet tenkte på robusthet men ikke sikkerhet. Nå kan vi ikke lenger stole på alle så vi må legge til sikkerhet på toppen

Pålitelighetsperspektivet - trusler mot pålitelighet:

Tre ting som kan gå galt - Fault, error og failure

Fault - før failure skjer det først en fault. Som at programvare har en bug feks. MEn da leveres tjenesten fortsatt.
Error - når en fault er aktivert. Denne feiltilstanden kalles error. Da oppfører systemet seg på en måte det ikke skal.
Failure - tjenesten blir ikke levert til bruker. Systemet klarer ikke å levere tjenesten.
En failure i et system kan føre til fault i et annet system som bruker denne tjenesten.
En bug kan ligge i mange år før det fører til en failure.

Random threats/trusler
Skjer uten menneskelig påvirkning. Ikke menneskeskapt
Tekniske software feil, tekniske hardware feil, naturkraft
Eksempler: fiberbrudd, ekstremvær

Unintentional (accidental) Threats

- Mellom random og intentional
- Skjer når mennesker gjør feil
- Mennesker er ofte det svakeste leddet
- Eksempler: sletter feil, sender noe sensitivt over mail, glemmer å oppdatere systemer

Intentional (malicious) threats

- Når mennesker med onde intensjoner utfører en handling
- Eksempler: spionasje, software angrep (malware, buffer overflow), sabotasje, social engineering (phishing, mennesker er lette mål og whaling, spesifikt mål)

Sårbarheter/Vulnerabilities

- Ingen trusler uten en sårbarhet. Man utnytter en sårbarhet for å angripe
- Kan være noe man vet om eller ukjent. Ofte dyrt å gjøre noe med de sårbarhetene vi vet om

- Eks, oljeplattform har sårbare systemer fordi de er gamle og ikke oppdatert. Har da en sårbarhet man ikke kan gjøre noe med fordi man ikke kan stoppe produksjonen eller ikke har noen bra erstatning som man vet vil fungere.

Kjernenettet er sårbart:

- Er mange aktører (service providers) involvert
- Mer sentralitet (less local autonomy)
- Mangler redundans, er mindre robust utenfor storbyene
- Er designet for å være robust, men er ikke alltid det i praksis. Problemet er mange aktører som kjøper seg inn hos hverandre, at kabler kan ligge i samme rør, og generelt at det er vanskelig å se om det er robust
- Mest vanlige grunner til å miste kobling er strømbrudd, linjebrudd, tekniske feil og unormalt stor trafikk
- Antenner kan være på samme tårn
- Tilgang til access nettverket er designet for normal trafikk, ved en krise kan store tjenester bli utilgjengelig for sluttbrukere.

Hvorfor er mange IKT systemer sårbare?

- Kompleksitet, åpne nett, opereres av mennesker, begrenset krav, begrensede ressurser, ny teknologi

Alvorlighetsgrad

Forskjell på teknisk alvorlighetsgrad og risiko

Teknisk alvorlighetsgrad

- Hva oppnår man med sårbarheten
- Hva skal til for å utnytte sårbarheten
- Standardiserte verdier for alvorlighetsgrad - CVSS

Risiko

- Avhenger av verdien til systemet og sannsynligheten for utnyttelse
- Kan representeres i en risikomatrise

Kjente sårbarheter

- Kan ha stor sårbarhet i noe som ikke er så viktig, da er det ikke så stor risiko
- Sårbarheter avdekkes hele tiden
- Når en sårbarhet er kjent er den lett å finne. Finnes nettsider for det. Derfor er det viktig å oppdatere så den ikke utnyttes
- Sårbarheter har stor verdi, derfor er det et stort marked for kjøp og salg av sårbarheter

Vi ruler!! <3 GOOO TEAM

Ukjente sårbarheter

- Vanskelig å beskytte seg mot
- Må bygge sikkerhet i lag

Ukjent til kjent sårbarhet heter Zero-day. Dette er veldig alvorlig.

Typer angrep

Tekniske angrep - målrettet eller opportunistisk

Målrettet

- Sett ut målet
- Vanskelig - dersom man har et oppdatert og robust system er det vanskelig å hacke seg inn fra internett
- Feilkonfigureringer eller svakheter - avhenger av dette i løsninger som er eksponert mot internett. Angrep mot påloggingssystemer er blandt de mest effektive
- Zero-day - svært effektivt å bruke, men veldig vanskelig å få tak i
- Eksempel: spear phishing

Teknisk opportunistisk

- La oss bare ta noen
- Enkle mål som er sårbare - enkle angrep mot systemer som allerede er sårbare
- Skannere - det finnes mange automatiske skannere som kontinuerlig skanner systemer på internett etter svakheter
- Enkle angrep etter kompromittering - kryptering av innhold, endring av reklame, referanser til andre sider for å øke Google score
- Eksempel: phishing

Trusselaktører

Script kiddie

- Ikke trent, utdannet
- Benytter kjente hacker verktøy
- Vanlig er DoS angrep, nedetid for systemer

Hackers

- Vet hva de gjør
- Finansielt motivert

Organiserte hackegrupper

- Avansert
- Stort fokus på å ikke bli oppdaget
- Bak kjente angrep
- Finansielt motivert, men større skala enn hackere

Vi ruler!! <3 GOOO TEAM

State Actors

- Stater, cyber avdelinger i land
- Mest avansert man kjenner til
- Utvikler egne angrep - skadevare og zero days
- Målet er informasjonsinnhenting og cyber krig
- Ofte vanskelig å knytte angrep og hendelser mot disse

Informasjonssikkerhet under COVID-19

- Enklere å gå inn på hjemmenett enn nettverk på jobben
- Bruk av VPN og hastverk kan føre til feil konfigurering
- Mange oppdaget at beredskapsplanen ikke var god nok
- Utfordringer med annen fysisk lokasjon - usikre hjemmenettverk, større sannsynlighet for å miste hardware, mer utsatt for phising
- Manglende vurdering av risiko - mange valg blir tatt uten at risiko er vurdert. Viktig å ikke hopper over dette.
- Tilgang - behov for VPN, alle skulle ha samtidig. Flere tjenester ble tilgjengeliggjort eksternt. Ny programvare og verktøy ble innført svært raskt

DEL 4 Sikkerhetsmekanismer

Må være forberedt på at ting kan skje.
Ulike tiltak:

- Administrative, tekniske (technical), fysiske (physical).

- Preventive (forebyggende), detective (identifisere og klassifisere en hendelse når den har oppstått), corrective (korrigerende. Begrense skaden).

Eksempler:

- Antivirus software: Preventive, detective og corrective control. Er en technical control.
- Finger scanner: Technical og physical. Preventive control (siden det brukes til å hindre folk i å komme inn i et rom f eks).
- Incident response procedure (prosedyre for hva som skal gjøres når noe skjer). Administrativ og corrective.
- Firewalls. Teknisk og preventive
- Access control. Teknisk og preventive
- Fire alarms. Fysisk og detective
- Security awareness training. Administrative og preventiv and/or detective

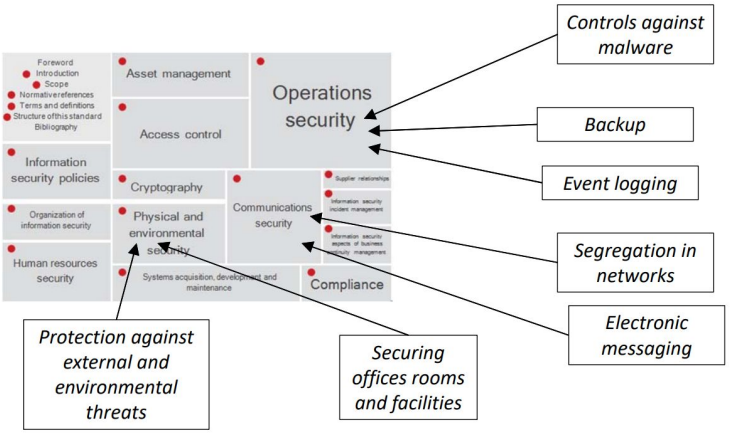
Vi ruler!! <3 GOOO TEAM

Autentisitet:

Autorisering: Tilgangsrettigheter når du har bevist at du er deg.

To steg:

1. *Identification* - presenterer en identifikator
2. *Verification* - viser tilknytning mellom identifikator og bruker



Identification demonstrates who you are, authentication how you can prove it and authorization what you are allowed to do.

Two different settings:
Kommer ann på hvem som autentiseres.

1. Data (or message) authentication. Hvilken maskin som dataen kommer fra. I IPsec sier man at man har data authentication, fordi man vet fra hvilken ip adresse dataen kommer fra. Men vet ikke da hvilken bruker som bruker den eller hvilken applikasjon. Proves where a piece of information is from. typisk implementert i nettverke eller transportlaget.
2. User (or entity) authentication. Hvem er det som bruker tjenesten, kommunikasjonskanalene? lenger opp i protokollstakken. Det er den man autentiserer. Typisk implementert i applikasjonslaget.

Ulike protokoller:

User authentication:

- Something you know. (Passord)
- Something you have. (Passport?)
- Something you are. (Finger print)
- Something you do. (Voice)
- Where you are. Location.

- Kan bruke fler på en gang: Multi-factor authentication.

Password weakness:

- Enkle passord. Enkle å gjette. Ordboksangrep.
- Skriver ned. Lett å finne. Bruker samme passord flere steder.
- Alle passord må lagres i et system. Kan angripes og deles

Password good practice:

- Lange passord. Flette inn sifre og ulike tegn. Store og små.
- Automatisk sjekk for svake passord.
- Hashing and salting the passwords. Ikke gjenlesbar i lagringen - modifesert.
- Account lockout.

Vi ruler!! <3 GOOO TEAM

- Lære bruker at det er viktig med avansert passord.

Eksempler på fysiske tiltak:

- Låse dører.
- Gjerder
- Kameraer
- Brannalarm
- ID kort

Eksempler på sikkerhetstiltak:

- Access control
- Anti virus software
- Backup
- Firewalls
- Intrusion detection system (IDS)
- Smartcards
- Spam filters (sorterer bort fishing emails osv)

Eksempler på administrative tiltak:

- Security policies
- Awareness training
- The "four-eye principle": Kritiske ting som skal skje? Kreve at to individuelle må logge inn før en patch kan rulle ut. Hindre at en person gjør noe galt. En annen sjekker.
- Se av hva man har.
- Rutiner og prosesser.
- Begrense hvem og hvor mange som har tilgang.
- Incident response procedures.

Viktig med komplett beskyttelse!!

Golden rules:

- Keep the key secret
- Protect the key from modification
- Know the importance of key length
- Generate a strong key
- Distribute the key securely

Kryptering:

En sikkerhetskontroll for å oppnå konfidensialitet for data

- Matematisk transformasjon der plain-text blir gjort om til en annen form, ciphertext. Kan reverseres - decryption.

Symmetrisk nøkkelkryptering:

- Samme (felles) nøkkel er brukt til å kryptere og dekryptere meldingene.
- Dårlig skalering - trenger ekstremt mange nøkler.
- Veldig rask fordi den bruker samme hemmelige nøkkel for kryptering og dekryptering

Symmetric (secret key) encryption

Asymmetrisk nøkkelkryptering:

- En privat og en offentlig nøkkel hver.
- Uansett hvor mange brukere, så trenger alle bare to nøkler hver.
- Skalerer bedre og gir bedre nøkkeldistribusjon - men er tregere.

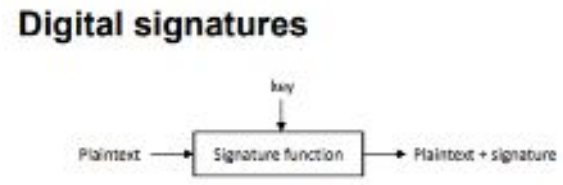
Asymmetric (public key) encryption

Vi ruler!! <3 GOOO TEAM

Begge typene kryptering er brukt i dag.
Må vurdere hva som trengs i systemet.
I praksis vil det ofte være en blanding (Hybrid approach).

Digitale signaturer:

- Vil være sikker på at en melding fra meg faktisk er fra meg
- Provide integrity, authenticity and non-repudiation.
- Gjøres med MAC.
- Sendes både melding og hash funksjon.
- Kan sammenlignes som et pass. Vanskelig å forfalske. En tredjepart som vi stoler på som har utstedt (Politiet). Certificate-issuing authority (CA). Inneholder også en digital signatur fra CA.
- Finnes mange CA-er. Er et Hierarki slik at ulike CA-er har sertifikat fra CA-er fra høyere opp. Root CA fungerer som tilliten i systemet og gir sertifikater til CAene under seg.
- Finnes ulike sertifikat standarder.
- Binder sertifikat til offentlig nøkkel (user, system og service).



Signaturfeltet i et digitalt sertifikat inneholder en digital signatur fra CA som har gitt ut sertifikatet.

Symmetrisk signatur. Delt hemmelig nøkkel brukes for å signere og verifiserer meldingen. Message authentication Code (MAC)

1. Avsender lager en MAC ved bruk av delt hemmelig nøkkel og fester den til meldingen
2. Avsender sender meldingen og MAC til mottaker
3. Mottaker verifiserer at MAC ble sendt med meldingen ved å bruke samme hemmelige nøkkel som lagde den.
   Den mest vanlige typen MAC er en Hashed Message Authentication Code (HMAC)

Asymmetrisk signatur. Bruker to forskjellige nøkler, en brukes til å lage signaturen og den andre brukes til å verifisere signaturen.

1. Avsender signerer meldingen med senders private nøkkel og fester den til meldingen
2. Avsender sender melding og digital signatur til mottaker
3. Mottaker verifiserer den digitale signaturen med med avsenderens offentlige nøkkel som hører til den private.

Vi ruler!! <3 GOOO TEAM

Sikkerhetsprotokoller:

IPsec:

- En protokoll suit som kjører på nettverkslaget.
- Gir konfidensialitet, integritet, authentication, replay-protection.
- Typisk brukt til å sette opp VPN.
- Provides data authentication, not user authentication.

TLS:

- Transport Layer Security. Lag 4 protokoll.
- Typisk brukt når vi browser på nett. Secure web-browsing. Https. File transfer, voice over IP.
- Bruker en PKI til å gi bruker verifisering.
- Symmetrisk nøkkel for konfidensialitet.
- Hybrid approach.

Application layer security:

- Sikkerhet beskyttelse implementert rett inn i applikasjonen

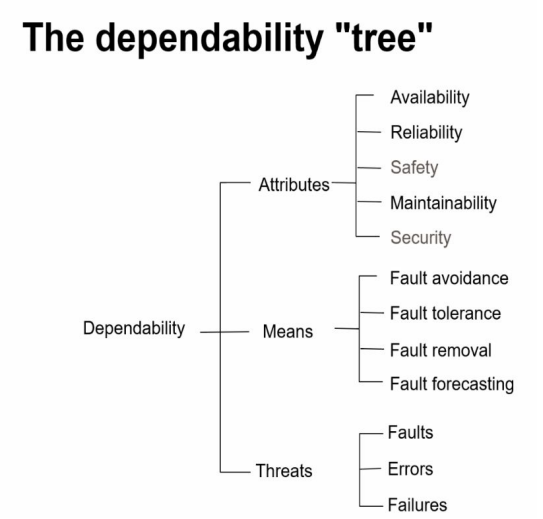
Mottiltak for dependability:
(Mottiltak: Hva vi kan gjøre for at et system er i stand til å levere sine tjenester).
Oppnå robusthet, pålitelighets perspektivet. Tiltak for å få systemet til å være oppe så lenge som mulig.

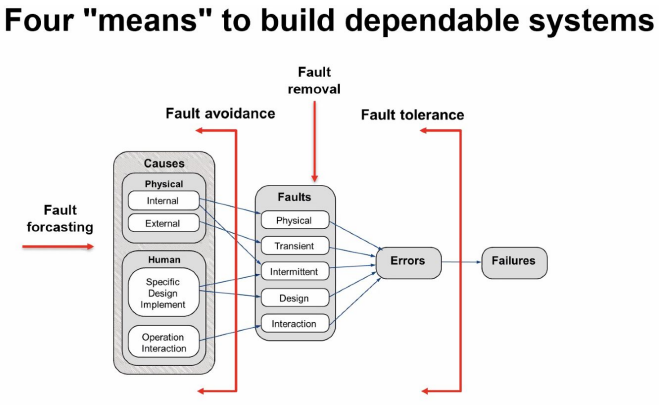
<u>Fire tilnærming- kategorier for å oppnå et pålitelig system:</u>

Fault avoidance: means to prevent the occurrence or introduction of faults.

Fault tolerance: means to avoid service failures in the presence of faults. A fault is allowed to produce an error, but the error is prevented to cause a failure

Fault removal: Means to reduce the number and severity of faults. During the development phase, fault removal involves three steps: verification, diagnosis, and correction. Fault removal during the operational life of the system consists of corrective and preventive maintenance.





Vi ruler!! <3 GOOO TEAM

Fault forecasting: Means to estimate the present number, the future incidence, and the likely consequences of faults.

(Både fault avoidance and fault tolerance har som mål å levere ønsket tjeneste på tross av forekomster av feil i systemet.)

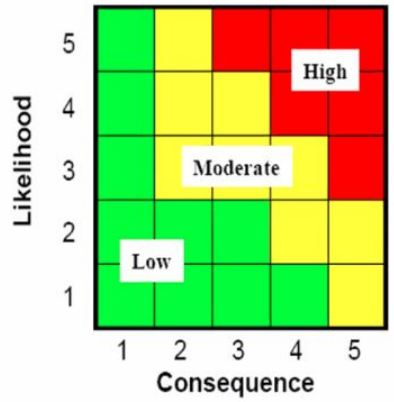
Fault dormancy - en passiv feil, en feil som ikke har fått betydning eller er utnyttet ennå.
Error latency - en feil som har inntruffet, men ikke er oppdaget eller har ført til en konsekvens.

Håndtere konsekvenser av fault og failure:
Kan velge å la systemet feile også heller ha en plan for å håndtere dette. Det gjør man ofte på grunn av kostnad.
Om det går galt og man skal få systemet opp igjen har man fire faser.

<u>Fire faser for å hente seg inn etter feil</u>
Eks strømnett

- Detection - noen ringer og sier at strømmen har gått
- Localization - finner ut hvor det gjelder
- Isolation
- Repair - restore

DEL 5 Risikohåndtering



Likelihood: Sannsynligheten for at en ting skjer.
Consequence: Innvirkningen en uønsket hendelse har på en verdi.
Risk level: Omfanget av risiko vurdert fra likelihood og consequence.

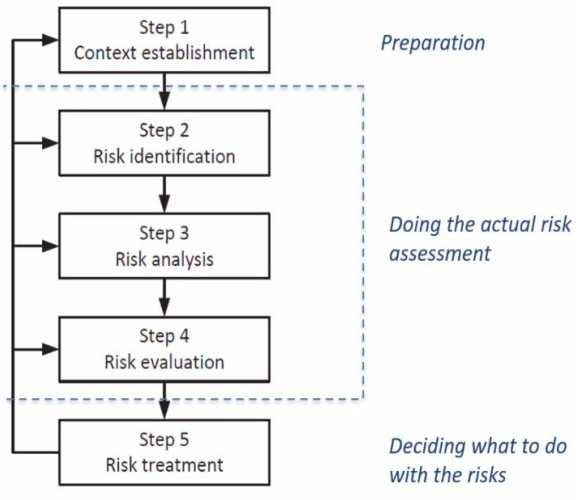
Likelihood value	Description
Rare	Less than once per ten years
Unlikely	Less than once per two years
Possible	Less than twice per year
Likely	Two to five times per year
Certain	Five times or more per year

Risikovurdering vs risikohåndtering
Risikohåndtering skjer hele tiden. Det jobbes med kontinuerlig. Risikovurdering gjør man innimellom. Feks en gang i året, eller når det er endring i system.

Vi ruler!! <3 GOOO TEAM

Finnes ulike faser for risikovurdering:

Step 1) Context establishment



- Goals and objectives. Hvorfor gjør man og for hvem gjør man risikovurderingen? (Kan være ulikt for ulike organisasjoner)
- Krav for noe vi ønsker å implementere. F eks. Skal vi innføre dette? Hva er risikoen hvis vi gjør det osv..
- Scope (Omfang): Hvilken del av systemet vil bli vurdert? Hva skal ikke bli vurdert? Hvilke aktører kan man stole på (trust boundaries)? Hvor blir systemet f eks angrepet? Hvilke mottiltak er allerede implementert?
- Risk scales: Må spesifisere hva man mener med 1,2,3.. Må vite hva som innebærer konsekvens 3.
- Risk evaluation: Sier hva som er akseptabelt. Det gule er det man bør gjøre noe med
- Etablering av kontekst. Inkluderer mål og hensikt med risikovurderingen, beskrivelse av omgang, identifisering av verdier(gjerne skille mellom primære og sekundære), skala for sannsynlighet og konsekvens, kriterier for evaluering av risiko (hva er akseptabelt og ikke)

Step 2) Risk identification

- Focus on the assets that you have identified! Make sure you are within the scope (of the risk assessment) that you have defined!
- Three methods to identify risks.
  *Interviews
  *Testing
  *Review of system documentation.
- Identifisering av riskio. Dette inkluderer identifisering av sårbarheter, relevante trusselaktører og uønskede hendelser, gjerne fra et brett spekter (angrep til tilfeldige feil)

Step 3) Risk analysis

- Mål: Estimere level på risikoen mtp likelihood og consequence.
- Lage matrise.
- Analyse av risiko. Dette inkluderer valg av sannsynlighet og konsekvens for de ulike hendelsene + argumentasjon for hvorfor en gitt sannsynlighet og konsekvens er blitt valgt.

Step 4) Risk evaluation

- Sammenligne risiko analyse med risiko kriterier for å kunne bestemme hvilke risikoer som skal få behandling.
- Rød - ikke akseptabelt. Gul - vurdere (kan være for kostbart).
  Grønt - akseptabel.
- Evaluering av risiko. Dette inkluderer visualisering av hendelsene i risikomatrise og identifisering av uakseptabel risiko (for eksempel gjennom plassering i rødt felt).

Vi ruler!! <3 GOOO TEAM

Step 5) Risk treatment

- Bestemme hva man skal gjøre med risikoen.
- Helst minske sannsynligheten for at ting skjer, men kan også minske konsekvensene. Kan minske for de som er i grønt også - for å gjøre det enda bedre.
- Håndtering av risiko. Dette inkluderer å velge (og argumentere for) strategier for å håndtere uønskede hendelser (redusere, fjerne, overføre eller akseptere). For risikoer som skal reduseres bør det foreslås fornuftige mottiltak

Fire strategier for å håndterte risiko:

1. **Avoid**
   Ved å stoppe aktiviteten som potensielt skaper risiko, eliminerer man sjansen for at det skjer problemer. Men ulempen ved dette er at man mister fordelene ved denne funksjonaliteten.

2. **Reduce**
   Hvis du ikke ønsker å ta bort aktiviteten helt, er en vanlig tilnærming å redusere risikoen forbundet med den.

3. **Transfer**
   Flytte risikoen et annet sted. F eks ved å kjøpe forsikring.

4. **Accept**
   Kan velge å akseptere risikoen. Spesielt hvis den ligger i grønt område. CEO har siste ordet på dette.

Kvantitativ vs kvalitativ risikovurdering:

- Kvantitativt risikovurdering: sette inn tall. Det er en 5% sjanse for at... Og det vil koste 3000 kr å kjøpe ny.
- Kvalitativ: Laptop tyveri er unlikely. (I disse notatene). Bruker unlikely, likely...

Utfordringer mtp risikovurdering i komplekse ikt systemer:

• Dagens IKT-systemer er svært store og komplekse.
• Økt informasjonsdeling og kontinuerlig integrering av ny teknologi.
• Trusselaktører kan oppholde seg hvor som helst i verden.
• "Insiders" er ofte de farligste trusselsaktørene.(Og det vanskeligste å forutsi og beskytte mot). Kan ikke alltid stole på personalet.
• "Dominoeffekten" er vanskelig å forutsi.
• Ingen har en fullstendig forståelse av "systemet".
• Informasjonen som er nødvendig for å vurdere konsekvens eller sannsynligheten har rett og slett aldri blitt samlet inn tidligere.
• Informasjonen er for vanskelig eller dyr å skaffe.

Vi ruler!! <3 GOOO TEAM

Risikohåndtering er en kontinuerlig prosess. Ongoing hele tiden.

Når bør man gjøre risikovurdering?

- På regelmessige tidsintervall. (f eks hvert år).
- Når et system endrer seg:
  Eks. en in-house server er flyttet til clouden.
  Eks. en ny service er tilbudt brukerne.
- Når miljøet rundt endrer seg, kan nye trusler dukke opp.

Pitfalls for risikovurdering:

- Mangel på fantasi.
- For mye tilrettelegging.
- Mangel på forståelse av hvordan systemet fungerer.
- Folk har et ønske om å være enige.

DEL 6 Redundans

Ekstra noder, linker, tid eller software. Redundans er tillegg av ressurser i form av hardware, software, informasjon eller tid som er forbi det som trengs for normal utføring av et system.

To måter å implementere redundans:
Modular redundancy: Har systemer som er identiske og aktive samtidig og deler opp mellom dem som gjør den samme oppgaven.
Standby redundancy (backup): Et aktivt system og et eller flere står som backup

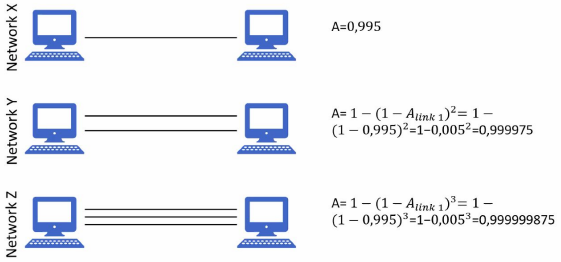
Ulemper med redundans, man får et robust system men:

- Det er dyrt. Trenger ekstra av masse
- Det øker kompleksiteten. Er flere komponenter som kan gå i stykker
- Kan se ut som man har det, også er det egt ikke redundant
- Vanskelig å vite når det er nok

Hvor mye redundans trenger man:
Kan regne på det og se om forskjellen er stor

Hvordan få redundans i:
Hardware - ekstra eller parallelle komponenter

You can use this to analyse the "value" of adding more redundancy



Vi ruler!! <3 GOOO TEAM

Software - management or fault handling software
Information - error-detection or error-correcting codes

DEL 7 Grafteori

Hvorfor gjøre strukturelle analyser med grafer?

- En graf er en forestilling av et reelt nettverk. Brukes for å forstå nettverk.
- Grafteori kan bli brukt for å se hvilke noder som er mest kritiske/sentrale. Hvor skal man investere mest ressurser.
- Finne ut hvilke noder som trenger høyere level av dependability.
- Fault-tolerance.
- Trafikkflyt og routing.
- En graf har noder og kanter - et nettverk har noder og linker. Vil analysere den nødvendige kapasiteten mellom linker.

Ulike strukturer i nettverk:

- Core - Mesh
- Metro - Ring
- Access - Tree

Nettside som forklarer de ulike:
https://www.guru99.com/type-of-network-topology.html#5

Network properties - Centrality:

Forskjellige sentraliserings mål - hvilken node er den viktigste/mest sentrale i hvert nettverk?

Degree centrality

- Node degree = centrality index
- Node med flest naboer er mest sentral
- Ulempe
    - Bruker kun lokal kunnskap
    - Node connection subgraphs are not recognized as important

Betweenness centrality

- Tegn den korteste pathen for alle node par. Hvor mange av de går gjennom v.

Closeness centrality

- Hvor nær er en node med alle de andre nodene

- Basert på summen av korteste vei mellom v og alle andre noder
- Lengden til de andre nodene

Robustness - Dependability in networks
How to assess dependability in a network?
Robustness

- Study impact of node/link removal
- Remove gradually nodes/links, study how network changes
- Assess network based on connectivity, centrality, maximum flow etc
- In network science: often Biggest component is used

Scale-Free networks - networks react very differently to random failures and targeted attacks

PENSUM ARTIKLER

Utfordringene med datasikkerhet:

- Kan være greit å sette krav, men mekanismen bak å møte disse kravene er kompleks.
- For å utvikle sikkerhetsmekanismer og algoritmer må man vurdere potensielle angrep på de sikkerhetsfunksjonene. Mange vellykkede angrep skjer fordi man ser på problemet på en annen måte og finner uventede svakheter.
- Det er bare når man ser forskjellige aspekter av en trussel at utdypende sikkerhetsmekanismer gir mening.
- Når man har designet flere sikkerhetsmekanismer er det nødvendig å bestemme hvor de skal brukes. Både fysisk som i hvilken del av nettverket, og logisk som i hvilket lag av TCP/IP.
- Sikkerhetsmekanismer inneholder mer enn en algoritme eller protokoll. Det kan også avhenge av en kommunikasjonsprotokoll som kan gjøre det vanskeligere å utvikle sikkerhetsmekanismer.
- Data og nettverkssikkerhet er en kamp mellom inntrengeren som prøver å finne et smutthull og designeren som prøver å lukke dem. Fordelen til angriper er at den trenger bare å finne et hull, mens designeren må finne alle for perfekt sikkerhet.
- Det er en naturlig tendens at brukere og system sjefer for lite fordeler av sikkerhet investeringer helt til en feil faktisk oppstår.
- Sikkerhet krever regelmessig og konstant monitorering og dette er vanskelig i dagens kort-tid, overbelastede miljø.
- Sikkerhet er fortsatt for ofte en ting som legges til etter et system er ferdig, istedenfor underveis i designprosessen.

OSI sikkerhetsarkitektur:

- Den som er ansvarlig for sikkerhet trenger noen systematiske veier til å kunne tilfredsstille sikkerhetskravene. Security Architecture for OSI definerer måter å gjøre dette på. Den er en vei for å organisere oppgaven om å tilby sikkerhet.
- OSI fokuserer på sikkerhetsangrep, mekanismer og service. De kan defineres som:
  - Security attack.
  - Security mechanism.
  - Security service.

1.3 Sikkerhets angrep - Security attacks:
En handling som kompromitterer sikkerheten ovenfor informasjonene som en organisasjon eier.

En nyttig måte å dele sikkerhets angrep inn i er passive og aktive angrep:
Passive:

- Prøver å lære fra eller bruke informasjon fra et system, men påvirker ikke systemets ressurser.
- Målet er å få tak i informasjon som blir sendt.
- To typer passive angrep er:
  - Utgi meldingsinnhold. Ting som sendes kan inneholde sensitiv eller konfidensiell informasjon. Vi vil hindre en motstander å få innsikt i det som blir sendt.
  - Trafikkanalyse. Dersom vi har kryptering kan en motstander fortsatt se lokasjon og identitet fra kommunikasjons hostene og observere frekvens og lengde på meldingene som blir sendt.
- Er veldig vanskelig å oppdage fordi de ikke inneholder noe endring av data. Ingen av partene i kommunikasjonen er klar over at det skjer.
- Det er mulig å forutse suksessen for slike angrep, ofte på grunn av kryptering. Derfor er det ofte vekt på å håndtere disse typer angrep med forebygging fremfor å oppdage de.

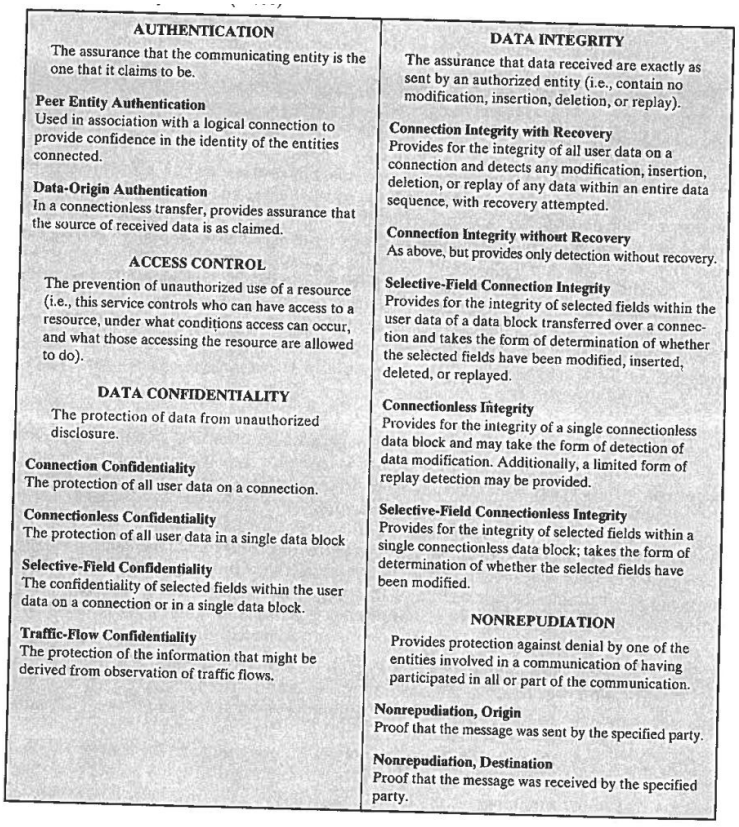
Aktivt:

- Prøver å endre systemressurser eller påvirker deres drift.
- Inneholder modifisering av datastrømmen eller å lage en falsk strøm med informasjon.
- Deles inn i fire kategorier:
  - Masquerade. Nå en enhet utgir seg for å være en annen.
  - Replay. Involverer passiv fangst av data og har en uautorisert effekt.
  - Modification of messages. En melding blir endret, forsinket eller om bestilt.
  - Denial of service. Forhindrer vanlig bruk. Kan ha spesifikt mål i slike angrep. Kan også være å overbelaste et helt nettverk.

- Lettere å oppdage, men vanskeligere å forhindre på grunn av en stor variasjon av måter å gjøre det på.
- Målet er å oppdage disse angrepene og recover etter de.

1.4 Security services:

- En service som er provided by a protocol layer of communication.
- En behandlings eller kommunikasjonstjeneste som tilbys av et system for å gi systemressurser en spesifikk type beskyttelse; sikkerhetstjenester implementerer sikkerhetspolitikk og implementeres av sikkerhetsmekanismer.
- Deler i fem kategorier;
- Autentisering: forsikre at en kommunikasjon er autentisk. Den det står at meldingen er fra, er den fra.
  - Peer entity authentication: for example two TCP modules in two communication systems.
  - Data origin authentication: sørger for bekreftelsen av kilden til en dataenhet. f eks elektronisk mail.
- Access control: Evnen til å minimere og kontrollere aksessen til vertssystemer og applikasjoner via kommunikasjonslenker.
- Data confidentiality: Beskyttelse av overført data. f eks over en TCP connection.
- Data integrity: connection-oriented integrity service håndterer streams av meldinger, og sikrer at meldingen er mottatt slik den er sendt, uten duplikasjon, insetting, modifikasjon, reordering .. osv. Integritet relateres til aktive angrep. Dermed er vi mer opptatt av detection istedenfor prevention.



AUTHENTICATION

The assurance that the communicating entity is the one that it claims to be.

Peer Entity Authentication
Used in association with a logical connection to provide confidence in the identity of the entities connected.

Data-Origin Authentication
In a connectionless transfer, provides assurance that the source of received data is as claimed.

ACCESS CONTROL

The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).

DATA CONFIDENTIALITY

The protection of data from unauthorized disclosure.

Connection Confidentiality
The protection of all user data on a connection.

Connectionless Confidentiality
The protection of all user data in a single data block

Selective-Field Confidentiality
The confidentiality of selected fields within the user data on a connection or in a single data block.

Traffic-Flow Confidentiality
The protection of the information that might be derived from observation of traffic flows.

DATA INTEGRITY

The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).

Connection Integrity with Recovery
Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.

Connection Integrity without Recovery
As above, but provides only detection without recovery.

Selective-Field Connection Integrity
Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.

Connectionless Integrity
Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.

Selective-Field Connectionless Integrity
Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.

NONREPUDIATION

Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

Nonrepudiation, Origin
Proof that the message was sent by the specified party.

Nonrepudiation, Destination
Proof that the message was received by the specified party.

1.5 Sikkerhetsmekanismer - Security mechanisms:

Mekanismene er delt inn i de som er implementert i spesifikke protokoll lag som TCP eller applikasjonslag protokoll, og de ikke er spesifisert til en spesiell protokoll eller sikkerhets service.
Reversible encipherment mechanism - en krypteringsalgoritme som tillater data å bli kryptert og dekryptert.

Vi ruler!! <3 GOOO TEAM

Irreversible encipherment mechanisms inkluderer hash algoritmer og melding autoriserings koder, som blir brukt i digitale signaturer og melding autorisering applikasjoner.

Table 1.3 Security Mechanisms (X.800)

SPECIFIC SECURITY MECHANISMS	PERVASIVE SECURITY MECHANISMS
May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.	Mechanisms that are not specific to any particular OSI security service or protocol layer.
Encipherment The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.	**Trusted Functionality** That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).
Digital Signature Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery (e.g., by the recipient).	**Security Label** The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.
Access Control A variety of mechanisms that enforce access rights to resources.	**Event Detection** Detection of security-relevant events.
Data Integrity A variety of mechanisms used to assure the integrity of a data unit or stream of data units.	**Security Audit Trail** Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.
	Security Recovery Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.

Table 1.3 Continued

SPECIFIC SECURITY MECHANISMS
Authentication Exchange A mechanism intended to ensure the identity of an entity by means of information exchange.
Traffic Padding The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.
Routing Control Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.
Notarization The use of a trusted third party to assure certain properties of a data exchange.

Relationship between security services and mechanisms:

SERVICE \ MECHANISM	Encipherment	Digital signature	Access control	Data integrity	Authentication exchange	Traffic padding	Routing control	Notarization
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

Four basic tasks in designing a particular security service:

1. Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose.
2. Generate the secret information to be used with the algorithm.
3. Develop methods for the distribution and sharing of the secret information
4. Specify a protocol to be used by the two principals that makes use of the security algorithm and the secret information to achieve a particular security service.

Dependability and performance in information and communication systems

1.1

Dependability og performance er ikke uavhengige properier. Et system med lav performace kan oppfattes som unavailable fra en brukers perspektiv.

Tekniske systemer blir beskrevet med to typer karakteristikker: funksjonelle og ikke-funksjonelle deler. Dette innebærer hvilke funksjoner som blir utført og hvor bra de blir utført.

Et bil eksempel: primærfunksjon er å transportere mennesker og ting fra et sted til et annet. Ikke-funksjonelle deler er kapasitet, maks hastighet, om bilen begynner og om den stopper på veien. Dette er performance (kapasitet og fart) og dependability (bilen starter og gjør sin jobb) properiene av systemet.

Model

Alle dependability og performance evalueringer av et system, enten om det er basert på matematiske analyser, simulering eller måling så avhenger det av en modell av systemet. Modellen er en abstraksjon fra det ekte eller prosjekterte systemet. En modell må både inkludere viktige detaljer for å representere systemet, samtidig som mindre viktige detaljer må utelukkes for å få til simuleringen på en rimelig tid.

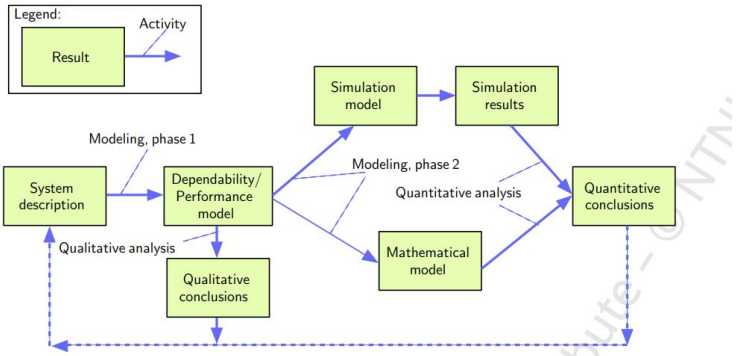


Figure 1.1: Modeling and analysis activities and results

Systemet

System - regularly interacting or interdependent group of items forming a unified whole, where an item may be a system, a subsystem or an atomic component.

Safe system is designed to prevent catastrophic incidents from happening while a dependable system is designed to provide high availability and/or reliability.

Vi ruler!! <3 GOOO TEAM

Når man skal utføre dependability og performance evaluering av et system er målet å identifiserer system componenter som begrenser dependability og/eller performance.

Struktur - strukturen til systemet reflekterer hvordan komponentene samhandler. Samhandlingene blir kalt oppførselen til systemet. Strukturen kan være fysisk (hvordan noder er koblet sammen), logisk (hvordan enheter koblet til en buss samarbeider), eller ingen av de.

Oppførsel

- kø disiplin (i mange systemer er det slik at hvis en ting er busy må de andre vente. FIFO, LIFO, prioritering)
- protokoller. Regler for deler av systemet. hvordan utveksle info, styre trafikk, gi error kontroll
- trafikk mekanismer. Routing algorithms. CAC and UPC.
- Fault-handling mechanisms. Omfatter error oppdaging, lokalisering og isolasjon. Forskjellige teknikker for å gi fault tolerance og fault removal.

Ulike typer komponenter - prosessor med prosesseringskapasitet (MIPS), hard disk med lagringskapasitet (Mbytes) og aksesstid (s) og transfer rate (Mbytes/s). Transmission channels som busser på innsiden av en prosessor.

The user and the environment

Hvordan omgivelsene påvirker systemet må også ses på.

Load profile- loaden som et IKT system må håndtere, også kalt trafikk. Er hvor ofte service requests blir mottatt og hvor lang tid det tar å serve den requesten. En korrekt beskrivelse av trafikk profilen er kritisk for en valid evaluering av systemet.

Trafikken observert i et IKT system er individuell flow fra mange brukere og avhenger av mange faktorer som:

- antall brukerer
- interessen og lokasjonene til forskjellige brukerer.
- type innhold. video eller annen web content
- variering i tid. daglig, ukentlig eller årlig.

Operation and maintenance

Operation og maintenance support sammen med logikk er viktige faktorer som må vurderes i mange dependability og performance problemer.

Trafikk load og vedlikehold aktiviteter påvirker failure rate.

Operation and maintenance functionality inkluderer:

- configuration control. forsikre seg om at det finnes nok transmission capacity mellom nettverksnoder så trafikk kan re rutes om en link feiler, noe som vil påvirke performance
- fault-handling. å oppdage når en ruter feiler og lokaliserer delen, om rute trafikk, fault removal (reparerer), restarte og teste fikset del. til slutt rute trafikk gjennom ruteren når alt er løst.

Vedlikehold
Når man skal håndterer fysiske feil er vedlikeholdsstrategiene å finne ut konsekvensene disse feilene har på påliteligheten til systemet og tjenesten det leverer. Mange faktorer spiller en rolle her.
Må ta hensyn til tiden det tar å fikse feilen (active repair time), tiden for å få deler (logistic delay) og tid det tar å sette i gang reperasjonen (administrative delay).
Vedlikehold er kostbart og dermed er strategien å minimere kostnad.

1.2 Quality of Service (QoS)

Tre forskjellige tolkninger: Vi bruker første i denne artikkelen

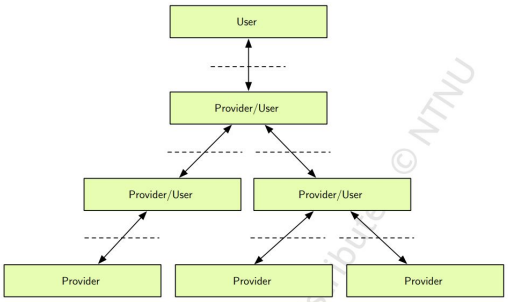
1. The delivery of a service in accordance with its specification. Denne definisjonen antar at hver tjeneste har sitt eget sett med QoS parametere og tilsvarende verdier. Som for eksempel availability større enn 99.9% og setup time mindre enn 200 ms osv.
2. The end-user satisfaction with a service. Relaterer det kun til brukeropplevelser.
3. The existence of mechanisms (in the network) for controlling the use of the different resources. Denne definisjonen har sitt utspring i arbeidet med å bruke Internett, dvs. IP-protokoll pakke for å håndtere tjenesteintegrert trafikk. Nettverket gir QoS ved hjelp av tjenestedifferensiering.

Definisjon - Degree of compliance of a service to the agreement that exists between the user and the provider of this service.

Bruker (User) - enhet som bruker en tjeneste sørget for av en annen enhet. Men trenger ikke være en end-user tjeneste.
Eksempel: transport protokollen er bruker av tjenesten sørget for av nettverk protokollen.

Tjeneste (Service) - et sett av funksjoner som tilbys på et interface mellom bruker og provider. Ikke nødvendigvis fysisk interface.

Compound systems
Vi kan dele på IKT systemer i mange brukere og providere i følge av lagene og segmentasjon av nettverket. Eksempel på lag er de forskjellige i ISO

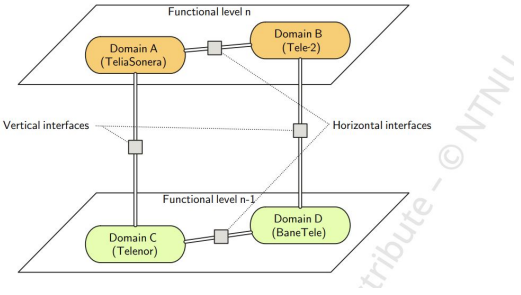


Vi ruler!! <3 GOOO TEAM

OSI modellen. I denne er et spesifikt lag en provider av en tjeneste for lagene over og brukeren av tjenesten sørget for av de underliggende lagene.

Hvis pålitelighet og trafikk mekanismene, og properties av alle provider/user assosieringen er kjent kan det i prinsipp være mulig å utlede Qos opplevelsen for end-user. Som Bit error rate på en transmission link, og quality of the speech av en menneskelig sluttbruker. Dette avhenger av hvordan informasjonen blir behandlet i nettverket med FEC og mistede pakker.

QoS i en commercial konteks:



Kravene til QoS are gitt av tolererte level av QoS parametere. Disse levelene er spesifisert i Service Level Agreement (SLA).
Denne er assosiert med et interface i et nettverk. Horisontale og vertikale.

Relation between dependability and performance
Are not independent of each other.
A system in which failures never occur but without sufficient resources to meet the performance requirements is not considered to be in a working state. Whether the performance requirements of a system are met or not determines whether the system is in a working state or not.
Et nettverk fungerer så lenge throutput ikke er 0.

To sum up, the QoS of a system is determined by the occurrence of errors, the performance with and without errors, and the operational condition the system is exposed to. Note that from the user's point of view the distinction between loss and unavailability may be unclear.

1.3 Use of modeling in development and dimensioning

Systemskostnaden påvirkes av dens pålitelighet og ytelse:

- Kostnadene for utvikling, produksjon, detaljhandel og garantier.
- Kostnadene ved anskaffelse og drift for tjenesteleverandører.
- Kostnadene ved kjøp, bruk og reparasjon.

Matematisk analyse:
Pros:

- I et velkjent problem kan resultat oppnås fort vha formler og algoritmer.

Cons:

- Kunnskapsnivået er høyt. Detaljerte modeller kan bli veldig komplekse.
- Modeller er ikke fleksible i tilfelle endringer i systemet.

Simulation:

Pros:

- Realistiske modeller kan bli brukt.
- Lavere level av kunnskap.

Cons:

- Tar lang tid.
- Usikkerhet rundt resultatene og vanskelig å tolke.

Measurements on (a prototype of) a system:

Pros:

- Resultatene er trustworthy, realistiske og detaljerte.

Cons:

- Kan kun utføres etter en eksisterende prototype er lagd.
- Vanskelig og dyrt å få til.
- Lang observasjonstid.

GJESTEFORELESNINGER

F13: Teknologi, trusler og utfordringer i kraftbransjen

(Se foiler)

Avhengig av dette fordi vi vil ha lys i lyspæren og vann i kranene. Ønsker en funksjonell by og samfunn. Digitaliseringen er enorm utover i samfunnet.

KraftCert

- Etablert i 2015 av nasjonal sikkerhet
- Statnett, Statkraft og Hafslund er eiere
- Jobber for bedre sikring i prosesskontroll-systemer ved å bistå kraftbransjen slik at de skal være oppdatert om relevante sårbarheter og trusler.
- Ikke opprettet for å tjene penger men for å hjelpe disse selskapene med digital sikkerhet.
- Ønsker å forminske skadeomfang ved angrep eller uhell.
- Deler informasjon, erfaringer og kompetanse.
- Identifiserer, analyserer og korrelerer sikkerhetshendelser.

Vi ruler!! <3 GOOO TEAM

Kritiske samfunnsfunksjoner:

- Kraftforsyning og elektroniske kommunikasjonstjenester.
- Ikt sikkerhet.
- Matforsyning.
- Fjernvarme.

Europeisk kraftmarked:

- Tettere samarbeid.
- Flere avhengigheter.
- Felles kraftmarked.
- Kraftbørsen: nordPool spot

Under vises en enkel og overordnet oversikt over hvilke infrastrukturer disse funksjonene er avhengig av:

IKT-sikkerhet	Systemer og registre, spesielt de som er klassifisert som «nasjonale felleskomponenter»
Matforsyning	Produksjonsanlegg, distribunaler, logistikksystemer, butikker
Drivstofforsyning	Raffinerier, havneanlegg, tankanlegg, bensinstasjoner
Vann og avløp	Vannverk, renseanlegg, pumper, høydebasseng, ledninger og rør
Finansielle tjenester	Finansiell infrastruktur
Elektrisk energi	Kraftverk, transformatorer, kraftnett osv.
Fjernvarme	Fjernvarmeanlegg, pumpestasjoner, ledningsnett
Ekom	Kjernenett, regionalnett, aksessnett, svitsjer
Transport	Veinett, jernbanelinjer, havner, terminaler, trafikkstyringssystemer
Satelittjenester	Satelitter, bakkestasjoner

Dette vil utgjøre en overordnet oversikt over hva som er kritiske infrastruktursystemer på et nasjonalt nivå

I NOU 2006:6 gis det en beskrivelse av hvilke kriterier som kan ligge til grunn for vurderingen av en infrastrukturs kritikalitet. De tre kriteriene er avhengighet, alternativer og (grad av) tett kopling.

Vannkraft/Vindkraft/Solkraft = Energiomforming.

- Turbin: Gjør om vann, vind, damptrykk til bevegelsesenergi.
- Generator: Tar bevegelsesenergien over til elektrisk energi.

Datatrafikk i kontrollsystemer er ofte statisk i motsetning til datatrafikk i forretningssystemer, det å få oversikt på hvilken trafikk som går hvor, er ofte greit – IDS kan være en del av et større system. Derimot kan konsekvensen av et vellykket angrep i kontrollsystem bli katastrofale.

Nøkkelelementer for å møte trusler:
• Gi mennesker og personell de rette forutsetninger
• Kjenn ditt nettverk og dine verdier
• Kontinuerlig sårbarhetsvurdering
• Deteksjonsmuligheter
• Hendelseshåndtering team(IRT)

Driftskontrollfunksjon: Alle organisatoriske, administrative og tekniske tiltak for å overvåke og styre anlegg i energiforsyningen.

(Felles) Sambandsplattform: Brannvesen, Kraftprodusent, Netteier.

F14: Teknologi, trusler og utfordringer i luftfartsbransjen

- Cyber sikkerhet er et relativt nytt konsept. har ikke blitt sett på som så relevant før.
- Men med økt tilkobling til forskjellige systemer, og økt bruk og deling av data gjør at trusselbildet blir større.

Vi ruler!! <3 GOOO TEAM

ATM: *Air traffic management* er et begrep som omhandler alle systemer som assisterer flyet fra det tar av fra en flyplass, er i luftrommet og lander på en ny flyplass. Er nødvendig for å kunne ha sikker og effektiv forflyttelse av flyet gjennom alle faser av operasjonen. ATM-sikkerhet oppnås ved å ha formelle regler for trafikk (avstand), kommunikasjonsteknologi, forhåndsbestemte flyplaner, radarsystemer etc.

ATC: *Air traffic control* er en service som skal forhindre kollisjoner mellom fly og andre gjenstander på en flyplass, og i tillegg sørge for en ordnet flyt av flytrafikken.

ANSP: *Air Navigation Service Provider* er en organisasjon som sørger for ATC. Dette kan være departementer, statlige-eide bedrifter eller private organisasjoner. I Norge er det Avinor som har denne jobben.

4D trajectory management: muligheten til å kunne kontrollere flyets luftbaner i fire dimensjoner, den fjerde dimensjonen er tid. Målet med 4D trajectory management er å sikre jevne baner og kunne fly den mest effektive veien, istedenfor å følge forhåndsinnstilte veipunkter. I tillegg skal det redusere avstanden mellom fly i lufta så flere fly kan være i luftrommet samtidig. Teknologier som muliggjør dette er ADS-B (Automatic Dependent Surveillance - Broadcast), CPDLC (Controller Pilot Datalink Communication) etc. ADS-C finnes ikke ennå, men vil bli lignende ADS-B bortsett fra at dataen ikke vil bli kringkastet, men bare sendt mellom flyet og en eller flere ATC ved forhåndsbestemte tidsintervaller.

ATM: Safety is achieved by

- Formal rules for control of traffic
- Communication technology - målet er å bytte ut den muntlige kommunikasjonen
- Pre-defined flight plans
- Radar systems
- Navigation systems
- Collision avoidance systems
- Air traffic controllers and pilot as human decision makers

ATM: dependability and performance
-Nødvendig for å oppnå safety

- All ATM systems are designed to fulfil pre-defined (high) reliability and performance requirements
- The ATM system are created through rigorous engineering prosesse.
- Safety assessment of ATM systems includes Hazard identification and risk assessment

Sårbarheter
Ingen autentisering over dagens VHF radio. Håndteres ved at man har en protokoll man kommuniserer etter. Inntrengere vil ikke vite om denne protokollen og gjenkjennes

Er ingen autentisering eller integritetsbeskyttelse på ADS.

Vi ruler!! <3 GOOO TEAM

Hardware to software:

- Flyprodusentene ønsker å spare vekt. Men strenge krav på redundans og separasjon. Derfor er det fristende å bytte til software - mindre vekt.
- Men software kan feile, er sårbart, og kan hakkes.

F15: Teknologi, trusler og utfordringer i Ekom

Generell oversikt

Nkom

- En etat underlagt kommunal og moderniseringsdepartementet.
- Ansvar for elektronisk kommunikasjon under her er Ekom

Ekomloven

- Lov om elektronisk kommunikasjon
- Handler om å sikre brukere i hele landet gode, rimelige og fremtidsrettede elektroniske kommunikasjonstjenester.

Ekoms rolle er å passe på at aktørene følger kravene i loven.
Det de gjør er:

- Konkurranseregulering
- Sikkerhet og beredskap
- Frekvens og spektrums forvaltning
- Utstyrskontroll og tilsyn
- Frekvens og spektrum monitorering

Nivåer av sikkerhet

Stat - handler om å ivareta Norges nasjonal sikkerhet. I hovedsak forsvaret.
Samfunn - samfunnssikkerhet. Det sivile sikkerhetssystemet styrt av sivilforsvaret og DSB. Alt fra skred, flom og ekstremvær.
Virksomhet - den enkelte virksomhet som Telenor og Telia. Hvilken som helst bedrift som må sikre seg mot digitale trusler.
Individ - hvor sikre vi føler oss som enkeltmenneske.

Totalforsvaret - knyttet til kriser. Samhandling mellom sivile og militære ressurser. Er forsvarets bistand til det sivile samfunn. Man kan ikke se på å forsvare landet uten tilgang til sivile ressurser. Det sivile forsvare har også behov for støtte fra militæret.

Fred, krise og krig

Når man bygger infrastruktur må man tenke at de skal fungere under alle disse. En sikker digital infrastruktur er en forutsetning i fred, krise og krig. Må ha visse planer og tanker om grunnleggende tjeneste i de mest ekstreme situasjoner.

Vi ruler!! <3 GOOO TEAM

Risikovurdering av ekomsektoren - Nkom publiserer hvert år en egen risikovurdering der de ser på hva som har skjedd og risikoer framover. Nevner 5G, korona og DNS-infrastruktur og BGP-ruting.

Nkoms verktøykasse for å bidra til en sikker digital infrastruktur

- Utvikle nytt regelverk, nye krav
- Tilsyn og sanksjoner
- Hendelseshåndtering
- Øvelser
- Utredning og analyser
- Økonomiske tilskudd

F16: Teknologi, trusler og utfordringer i olje og gass

Hvis noen vil ramme energi sikkerheten i Europa kan man gå etter Norge fordi det også rammer Storbritannia, Frankrike, Nederland og flere. Norge er 3. størst på gass og 15. størst på olje.

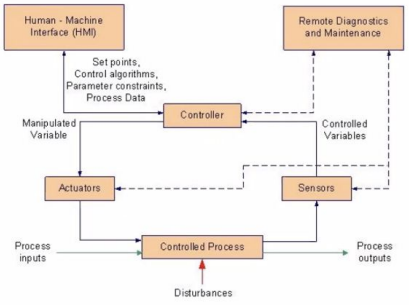
Petroleumsproduksjon er delt i tre

- Upstream: Leting etter og produksjon av olje og gass
- Midstream: Transport av hydrokarboner og lagring
- Downstream: Raffinering og fordeling til sluttprodukt

Konsekvens bildet - Det man er redd for er tap av liv, tap av produksjon og skader på miljø
Prinsipper for beskyttelse - Aldri slipp olje og gass ut. Hold folk trygge. Beskytt brønnen. Beskytt utstyret.
Barrierestyring - risikostyring. Vil ha mottiltak som reduserer sannsynligheten for uønskede hendelser eller begrense konsekvenser ved uønsket hendelse.
Safety Instrumented Systems - systemer som kun forhindrer ulykker. Feks brannslukking. Siste mekanisme før det går skikkelig galt.
ICS - Industrial Control Systems. Industrielt styringssystem. Brukes i all industri. Består av hardware, software og protokoller. Men spesialiserte.

ICS vs IT
Stiller krav til at det ikke tar så lang tid før man får svar. Ikke så høyt krav til båndbredde. Ting må være konstant.

ICS	IT
Sanntid	Ikke-sanntid
Respons et tids-sensitivt	Respons må være på lik form
Medium båndbredde	Høy båndbredde
Varierende ping-tid er ikke akseptabelt	Varierende ping-tid kan være akseptabelt



Cyberangrep på industrielle styringssystemer

- *Stuxnet* - gikk konkret etter styringssystemet, og spesifikt etter underjordisk anlegg.
- *Crashoverride* - Første kjente skadevare for å angripe strømnett. Angrep på sivil infrastruktur.
- *Triton/Trisis* - går konkret etter system instrumental system så disse feiler og ikke hindrer hendelsen.

Digitalisering av petroleumsbransjen
Har fått helautomatiserte plattformer. Styres fra land, 3 uker i måneden og vedlikehold siste uken. Kontrollrommet er flyttet på land på noen plattformer også. Men har brukt IT i lang tid i petroleum.
Digitalisering fører til større angrepsflate. Når man kobler flere ting sammen får man flere veier inn.

Sårbarheter på norsk kontinentalsokkel:

Lysneutvalget - NOU 2015:13 Digital sårbarhet – sikkert samfunn

1. Manglende oppmerksomhet på og opplæring i digital sikkerhet hos ansatte
2. Fjernarbeid i forbindelse med drift og vedlikehold
3. Bruk av standardprodukter med kjente sårbarheter i produksjonsmiljøer
4. Mangelfull sikkerhetskultur i forbindelse med digitale sårbarheter hos underleverandører
5. Utilstrekkelig separasjon av datanett
6. Bruk av mobile innretninger og lagringsenheter, inkludert smarttelefoner
7. Datanett mellom landinstallasjoner og oljefelt
8. Manglende fysisk sikring av datarom, koplingsskap, m.m.
9. Sårbar programvare
10. Utdaterte styringssystemer på anlegg

Sårbarheter i industrielle styringssystemer:
- Lite eller ingen innebygd sikkerhet
- Et skille mellom nyerer og eldre systemer
- Det aller meste er gammelt. Har ikke støtte for integritet eller konfidensialitet. Kan ikke fikses heller. De eldre enheter forstår bare noen konkrete kommandoer.
- Tiltak som brukes i IT kan ikke nødvendigvis brukes i ICS.

Utfordringer for cybersikkerhet i olje og gass:
- Isolert miljø og lite teknisk kompetanse on-site
- Langt livsløp på utstyr og komponenter, til dels utdaterte styringssystemer
- Ekstremt kompliserte avhengigheter og hundrevis av leverandører

Avhengigheter til annen kritisk infrastruktur
- Elektrifisering av produksjon og plattformer. Koblet til strøm på land. Avhengig av at den er stabil.

- Telekommunikasjon/Fiber. Nødvendig for å ha kontrollrom på land. Ringstrukturer for redundans.

Hvordan arbeide med sikring?
Defence in depth - beste praksis for sikring mot cyberangrep

- Du vil aldri være fullstendig beskyttet med et lag med beskyttelse
- Innføre flere lag med sikkerhetskontroller/mottiltak
- Preventive tiltak - reduserer sannsynligheten til en uønsket hendelse
- Reaktive tiltak - reduserer konsekvens av uønsket hendelse.

MTO - Menneske, teknologi, organisasjon. Om man vil hindre adgang til et rom. Kan da ha tekniske elementer som gjerder og kode. Må også ha vakter og ansatt. I tillegg til det operasjonelle, rutiner på hva man skal gjøre om noe går galt.
Standarder og veiledning er gode ressurser.

F17: Hendelseshåndtering og beredskap

Prosess for hendelseshåndtering:
Handler om at når man gjør det, så er det essensielt å gå gjennom en planleggingsfase, hvor man går gjennom ulike scenarioer som kan skje.

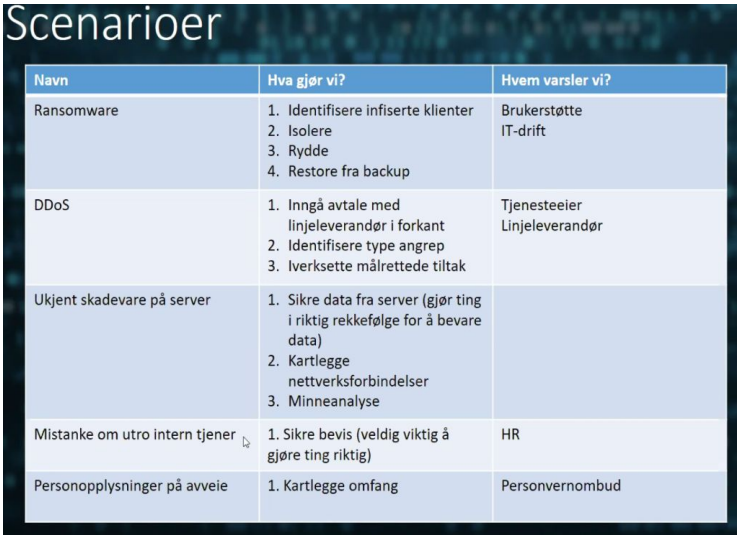
- Vil stille mer forberedt neste gang.
- Hva må på plass for å respondere på en hendelse.
- Hva slags hendelser skal planen kunne dekke?
- Mange elementer å holde styr på. Kan være lurt å ha en varslingsliste klart på forhånd, så blir det ikke så mye stress når hendelsen først inntreffer.

Beredskap:

- Bestemme rutiner for når ting skjer.
- IT, Sikkerhet, Beredskap (brann osv).

Prosessnett:

- Styrer fysiske prosesser (lyskryss, signaler på jernbane)
- Annet sikkerhetsnivå. Har vært separert med it-drift. Men er mer kommunikasjon over IT nå.



Trusselaktører:

- Ulike aktører må håndteres på ulike måter.
- Angripere som er målrettet vil kunne bruke mer ressurser for å få til det de vil.
- Vurdere hvilke aktører man kan møte. (ferdigheter, ressurser, overordnet mål, hvor opptatt de er av opsec - å holde seg skult)

Vi ruler!! <3 GOOO TEAM

- Skille på interne og eksterne.
- Statlige, Profesjonelle, Målrettede opportunister, Opportunister.

Hensikter:

- Minimere konsekvenser av hendelser
- Redusere stress
- Redusere avhengighet av enkeltpersoner. Jo flere som kan, jo mindre avhengig er vi av én person f eks.
- Lage prosedyrer og rutiner
- Motvirke "analyst bias". (Kognitive biases)

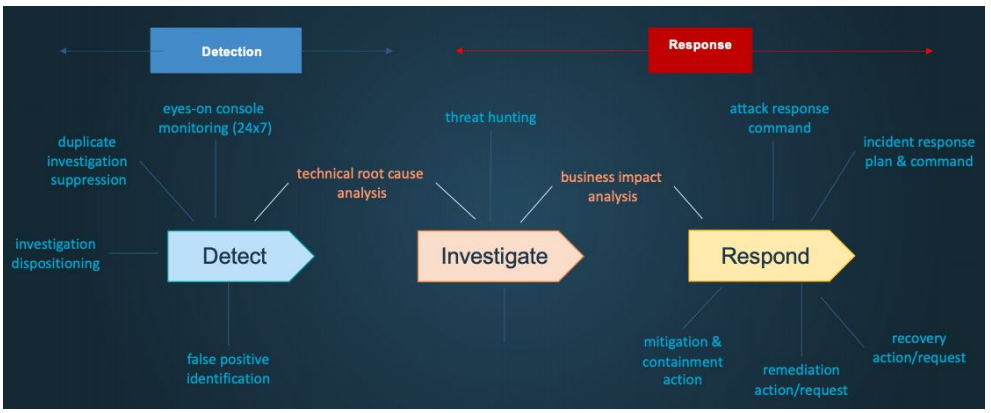
CASE fra forelesning:

- IDS-alarm gikk - skadevare oppdaget. Kinesisk skadevare.
- Selskapet begynte å reinstallere klienter og servere infisert med skadevare, og blokkere kjent IP-adresse (var det som var prosedyren).
- Problem løst?
- Mnemonic fikk i oppgave å se om problemet faktisk var løst. Fant ut at aktøren sannsynligvis hadde vært tilstede i flere måneder. Aktør hadde eksfiltrert sensitiv data gjennom skadevaren gjentatte ganger. Aktør holder seg skjult lenge før de oppdages.

F18: Hendelseshåndtering og beredskap - Security Operations Center

- Insight: Know your assets. Kunnskap.
- Prevention: Forebygg for farer. Å låse dører er en fin start.
- Detection: Oppdag fort. Bruk powerfull AI and world-class SOCs.
- Response: Hvert minutt teller. Handle raskt.
- Recovery: Vær sikker på at selskapet er up and running fort.

SOC relies upon our joint ability to leverage people, processes, and technology to improve our clients' maturity posture throughout all phases of the SOC lifecycle.



Vi ruler!! <3 GOOO TEAM

F7: Teknologi, trusler og utfordringer i maritime

- Transport regnes som en av seks kritiske infrastrukturer i Norge
- Sjøveien er avgjørende som ferdselsåre for personer og gods
- Shipping blir mer og mer digitalisert, som også gjør det mer følsomt mot angrep. Eks pirater, smugling, hackere, spionasje

Hvorfor er shipping avhengig av IKT?
- Skipene blir mer og mer komplekse
- menneskelig kraft koster mer enn automatisert
- generell mangel på sjøfolk

Unikt med shipping innen IKT
- har begrenset antall enheter
- lang levetid
- begrenset tilgjengelighet
- internasjonal industri
- mange aktører

Noe av det viktigste når det gjelder sikkerhet er **kostnad vs nytteverdi**
Det er viktig å kartlegge reelle behov og finne riktig løsning. Må være kostnadseffektivt, brukervennlig, ikke konkurransevridende og implementerbart på tvers av industrien.

DEL 8 - VDES CASE oversikt

- Norge har alltid vært avhengig av sjøen og havet.
- Sjøveien er avgjørende som ferdselsåre både for personer og gods
- Internasjonal handel er viktig for norsk økonomi

- I dag har skip begrensede muligheter til datakommunikasjon under transport på åpent hav. Begrenset båndbredde - høyt pakketap.
- Mannskap har lite IT kunnskap.
- Vanskelig å anskaffe nytt utstyr hvis det feiler - stiller høyt krav til utstyr.
- Mer funksjonalitet og økt effektivitet - nye sårbarheter og ondsinnede aktører.
- Kommende teknologisk utvikling - VDES (VHF Data Exchange System):
  - Gi skip datakommunikasjonsforbindelse med høyere hastighet.
  - Økt pålitelighet (mindre pakketap).

- Lavere kostnad for pakkene.
- Konstellasjon av satellitter som gir skipene internett tilkobling overalt.
- Tilbyr tre delsystemer: AIS, ASM(meldingsformat), VDE(Kommunikasjonskanal).

Behovet for sikkerhet øker når flere tar i bruk VDES. Dette caset tar for seg to applikasjoner:

- **Trafikkovervåkning**. Vil bli kringkastet ("broadcast") mellom skip ("ship-to-ship") med hjelp av delsystemet AIS, over radio
- **Skipsrapportering**. Vil bli sendt fra skip til havnemyndighetene ("ship-to-.shore") med hjelp av delsystemet VDE, enten over radio eller satellitt.

Liste over verdier i VDES:

- Informasjonsverdier:
  - AIS meldinger (brukes i applikasjonen "route exchange")
  - Digitalt FAL-skjema (brukes i applikasjonen "ship reporting")
- Tjenester
  - Broadcast av AIS meldinger (dette er en tjeneste som VDES radioen leverer: den vil sammenstille og sende ut AIS meldingene automatisk)
  - Display av AIS informasjon på kart (dette kan sees som en tjeneste som ECDIS:en tilbyr)
  - Webbasert tjeneste for mottak av digitale FAL rapporter. Leveres av havnemyndighetene
  - SATCOM forbindelsen (dette kan sees som en tjeneste som tilbys av satellitt-nettverket og som brukes av VDES radioen på skipet for VDE kommunikasjon ship-shore)
  - GNSS basert posisjonering (dette kan sees som en tjeneste som tilbys av GNSS utstyret på skipet)
- Fysiske verdier:
  - VDES radio (installert på skipet)
  - VDES antenne (installert på skipet)
  - GNSS antenne (installert på skipet)
  - ECDIS monitor
  - VDES shore station (installert på land)
  - VDES satellitten (sannsynlig at dette er out of scope)
- Andre typer komponenter
  - Database for lagring av FAL rapporter som er mottatt av havnene
  - Software for generering og innsending av FAL rapporter. Installeres på brua på skipet
  - ECDIS software, Installeres på brua på skipet
  - Database for lagring av historisk AIS data
  - Bro-nettverket på skipet (internt nettverk som kobler sammen utstyret på skipet)

Vi ruler!! <3 GOOO TEAM

Potensielle trusselaktører:

- Terrorister
- Konkurranse
- Kriminelle ute etter penger
- Hackers som vil vise skillz og få oppmerksomhet

Begreper:

Bacon nummer - en måte å representere hvor sentral en node er. Hvor sentral har ofte noe med hvor robust det er også.

Service level agreement (SLA) - I tillegg til mange aktører er det mange tjenester på toppen av det. De bruker disse avtalene for å samarbeide og bruke tjenester av hverandre. SLA sier noe om kvaliteten til tjenesten som leveres. Hvem som har ansvar for hva. Skjer når man godtar brukervilkårene. Eks, skal du bestille ferie så bruker booking.com banktjenester. Tjenester henger sammen.

Bug bounty - selskaper lar alle eller inviterte fritt teste systemene deres. Må da rapporterer det man finner på en ryddig måte. Kan få store pengepremier.

Accountability: digitale handlinger skal kunne spores tilbake til de som har utført den. Muligheten til å kunne stille folk ansvarlig for handlinger de har utført.

Non-repudiation: forsikrer beskyttelse mot benektelse fra en av de involverte partene/enhetene i kommunikasjon om å ha deltatt i hele eller deler av kommunikasjonen. Ikke-fornekting forhindrer derfor enten avsender eller mottaker fra å nekte å ha bidratt i kommunikasjonen.
Kan ha et større omfang enn bare kommunikasjon, betyr at en digital handling ikke kan nektes for i etterkant.

Fail-safe design: Sikre at hvis systemet failer, så failer det ikke katastrofalt slik at konsekvensene er enorme, men prøver å gjøre slik systemet failer på en kontrollert og akseptabel måte.

Black swans: Risikovurdering som er vanskelig å forutse. Noe som er ekstremt lite sannsynlig. Kan ikke tenke seg til at noen f eks ønsker å gjøre noe så sykt. F eks 9/11. Man plukker ikke opp slike ting like ofte i en vurdering som f eks at en server blir ødelagt.

Vi ruler!! <3 GOOO TEAM

“Support systems” i ikt systemer: Er til for å finne og rette enkle feil. Handler om at systemet blir mer komplekst, og kanskje vanskelig å håndtere kritiske feil. Less human effort needed - but more advanced human effort needed.

STRIDE: En modell av trusler for å identifisere datasikkerhetstrusler. Ulike kategorier av trusler: spoofing, tampering, repudiation, information disclosure, denial of service, elevation of privilege.

MTFF: Mean time to first failure. Kan sette ikke-funksjonelt krav med dette. Går under dependability:reliability.

Computer security: The protection afforded to an aoutmated information system in order to attain the applicavle objectives of preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/data and telecommunication)

Real time requirement for user interactions = approx. 100ms. I.e the end to end delay.

Stakeholders: A stakeholder is a party that has an interest in a company and can either affect or be affected by the business. The primary stakeholders in a typical corporation are its investors, employees, customers, and suppliers. Eksempel på stakeholders: The product owner, an end-user, a developer, someone from IT operations, a lawyer, a secretary, a facilitator, …

Når er fault avoidance en bedre strategi enn fault tolerance?
Fault avoidance: Bugs in the data routing and priority function may have severe consequences. The software should therefore be carefully designed and implemented, aiming to have a fault free component. Fault tolerance: Space radiation sometimes causes bit errors in the satellite connection. This is a type of fault that is difficult to avoid. The satellite connection should therefore be fault tolerant.

Humans are the weakest link - Low usability of security mechanisms. Employees are not trained in security. Conflicts between completing work related tasks in time and following security policies.

DDoS: A DDoS attack in an attack where the perpetrator tries to make a machine or network resource unavailable to its intended users by flooding the targeted machine or resource with superfluous requests from many different sources, hence preventing legitimate requests from being fulfilled.

"Pretty Good Privacy": A protocol for protecting email communication.

Vi ruler!! <3 GOOO TEAM

Watering hole attack: Infection through a website that the target users are known to visit
User-provider relationship eksempel: Mobilabonnement eier (user) - Telenor (provider). Telenor (user) - Subcontractor (provider)

Traffic Light Protocol: To define how to share sensitive information amongst organisations.

"zero-day vulnerability”: A vulnerability, which is unknown to those who are working on mitigating vulnerabilities.