



IFI

komprimierte 2120 notater

/BLASTBLASTBLAST

Første siden her er kun en oppsummering fra oppsummerings-slides

- **Kontrollmetoder:** DAC (identitetsbasert), MAC (merkebasert), RBAC (rollebasert), ABAC (attributtbasert).

Sikkerhetstyper

- **Fysisk sikkerhet:** Beskytter utstyr mot innbrudd og tyveri.
- **Samfunnssikkerhet:** Sikrer funksjonalitet i kritisk infrastruktur.
- **Sivil og rettssikkerhet:** Opprettholder lov og orden.
- **Personalsikkerhet:** Beskytter liv og helse.
- **Miljøsikkerhet:** Forhindrer forurensning, ivaretar natur.
- **Informasjonssikkerhet:** Beskytter informasjonsverdier mot skade.
- **Personvern:** Sikrer lovmessig håndtering av personopplysninger.

Informasjonssikkerhet

Sikkerhetsmål (KITPAUS)

- **Konfidensialitet:** Beskytter mot uautorisert tilgang (f.eks. kryptering).
- **Integritet:** Hindrer uautorisert endring av data (f.eks. hashing).
- **Tilgjengelighet:** Sikrer tilgang til data/tjenester når nødvendig (f.eks. redundans).
- **Uavviselighet:** Sørger for at handlinger kan spores til brukeren (f.eks. digitale signaturer).
- **Sporbarhet:** Lar handlinger spores tilbake til ansvarlige.
- **Personvern:** Beskytter personopplysninger i samsvar med GDPR.

Sikkerhetstiltak

- **Pålitelighet:** Systemer skal fungere korrekt, også med visse feil.
- **Autentisitet:** Bekrefter at brukere/systemer er ekte.
- **Tilgangsautentisering:** Sikrer at kun autoriserte brukere får tilgang.
- **Tilgangsautorisering:** Spesifiserer hvilke ressurser brukere har tilgang til.
- **Tilgangskontroll:** Bruker regler for å styre tilgangen basert på autentisering og autorisering.

Risiko og trusselhåndtering

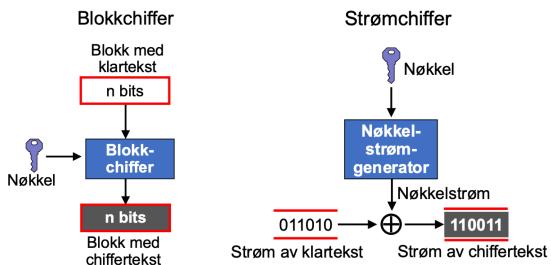
- **Risiko:** Avhenger av verdi, trussel og sårbarhet.
- **Sikkerhetstiltak:** Forebyggende (f.eks. kryptering), oppdagende (f.eks. IDS) og korrigende tiltak (f.eks. backup).
- **Sikkerhet for data i ulike tilstander:** Under lagring, overføring og bruk – beskyttes med tilgangskontroll og kryptering.

Tilgangskontroll

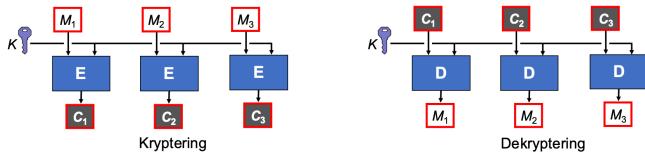
- **Autentisering:** Sikrer at brukere/systemer er de de utgir seg for å være (f.eks. passord, 2FA).
- **Autorisering:** Spesifiserer hvem som har tilgang til hvilke ressurser.

Kryptografi

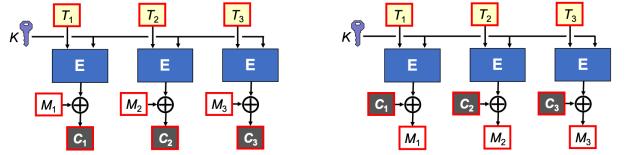
- Skjule betydningen av en melding
- Brukes for KIT, digSig, og PKI
- Kryptering:
 - $C = E(M, k)$
 - Chiffer = Encryption(Message, key)
- Dekryptering:
 - $M = D(C, k)$
 - Message = Decrypt(Chiffer, key)
- Chifferstyrke er basert på nøkkelstørrelse
 - f.eks 256 Bits
- Symbolfrekvens for tidligere chiffer ført til:
 - Nye løsninger
 - Blokkchiffer (Vanligste type i dag)
- DES, svak/utdatert, AES nøkkelstørrelser på 128, 192, 256.
- Blokkchiffer:



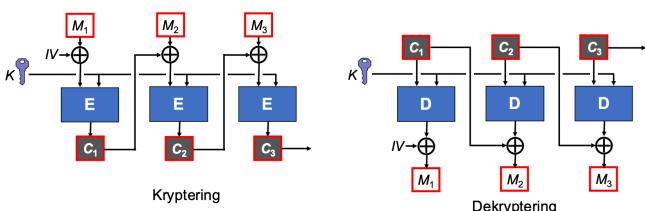
- ECB - Base blokkchiffer



- CTR Counter mode (teller med i kryptering)



- CFB Block chain (forrige blokk med i neste)

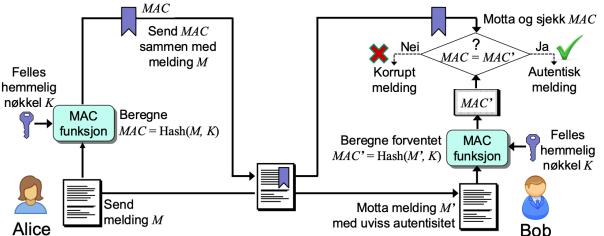


- CBC, DFB etc...

Hash

- **Lett å beregne**
- **Komprimerende til fast størrelse**
- **Enveis**
- **Sterk kollisjonsresistens**
- Kjente hashalgoritmer
 - MD5, 128 bits
 - SHA-1 160 bits
 - SHA-2 256, 384, 512 (sikker)
 - SHA-3 (lite brukt pga SHA-2)
- Meldingsautentisering med MAC
 - MAC = Hash(M, k)

Meldingsautentisering med MAC



- Krever kjent nøkkel
- **ENKEL**, ikke uavviselig

Symmetrisk vs. Asymmetrisk kryptografi

Symmetrisk kryptografi:

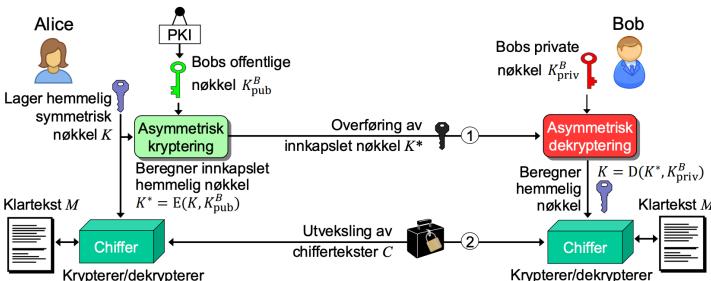
- Bruker én felles hemmelig nøkkel for både kryptering og dekryptering.
- Rask og effektiv for store mengder data.
- Nøkkeldeling er krevende i åpne nettverk.
- Vanlige algoritmer:
 - **AES:** Standard for sikkerhetskritiske applikasjoner.
 - **3DES:** Bruker DES tre ganger, men er tregere og mindre brukt.
 - **Blowfish:** Egnet for begrensede ressurser, men ofte erstattet av AES.

Asymmetrisk kryptografi:

- Bruker to nøkler — en offentlig for kryptering og en privat for dekryptering.
- Ressurskrevende, derfor kombinert med symmetrisk kryptering i hybrid kryptering.
- Vanlige algoritmer:
- **RSA:** Sikker, men krever store nøkler (2048 bits).
- **ECC (Elliptisk kurvekryptografi):** Gir samme sikkerhet med mindre nøkler (256 bits) ved bruk av elliptiske kurver og diskrete logaritmer.

Hybrid kryptering

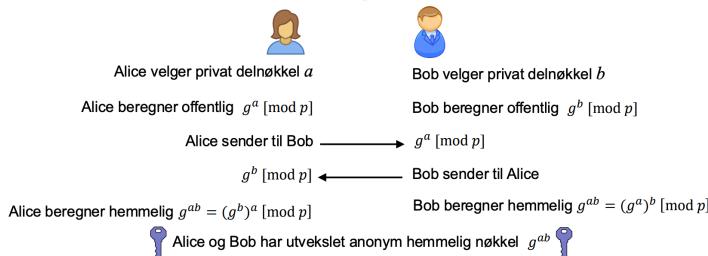
Hybrid kryptering (gir ikke fremoverhemmelighold)



- **Symmetriske chiffer:** Brukes til data-kryptering på grunn av hastighet.
- **Asymmetriske chiffer:** Brukes til nøkkeldistribusjon for å sikre kommunikasjon.
- **Svakhet:** Mangler perfekt fremoverhemmelighold, men dette kan oppnås ved bruk av **Diffie-Hellman**.

Diffie-Hellman nøkkelutveksling

Diffie-Hellman nøkkelutveksling



- Utveksler en felles hemmelig nøkkel mellom to parter.
- Sikrer fremoverhemmelighold — kompromitterte nøkler påvirker ikke tidligere økter.
- Ingen innebygd autentisering, sårbar for man-in-midten-angrep.
- **Bruksområder:** TLS (HTTPS), IKE, IPSec.

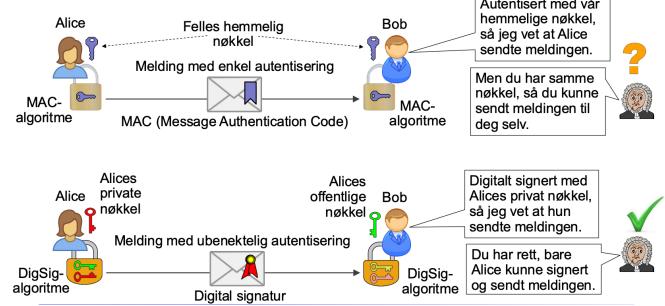
Digital signatur

- **Begrensning med MAC:** Kan ikke brukes til autentisering som kan verifiseres av tredjepart.
- **Digital signatur:** Gir ubenektelig autentisering; kan verifiseres av en tredjepart.
- Funksjoner:
 - **Signering:** Utføres med privat nøkkel.
 - **Verifisering:** Utføres med offentlig nøkkel.

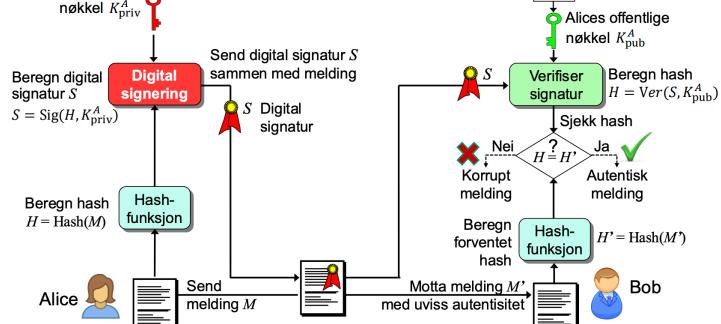
Kvantecomputere og kryptografi

- **Qubits:** Kvantedatamaskiners grunnlag, som øker regnekapten dramatisk.
- Risiko for kryptografi:
 - **Symmetrisk kryptering:** Fortsatt relativt trygg med økte nøkellengder.
 - **Asymmetrisk kryptering:** Potensielt truet; kvantedatamaskiner kan teoretisk bryte algoritmer som RSA og ECC, hvilket vil kreve nye, kvantesikre algoritmer i fremtiden.

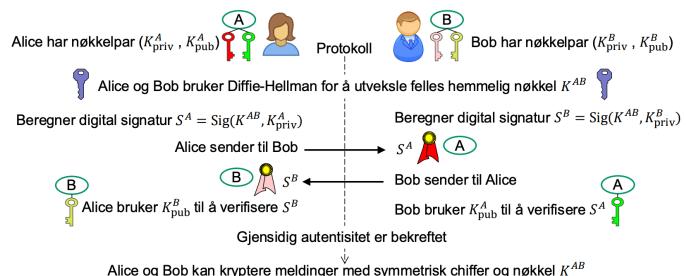
Enkel eller ubenektelig meldingsautentisering



Praktisk digital signering



Autentisert nøkkelutveksling for fremoverhemmelighold



Systemsikkerhet

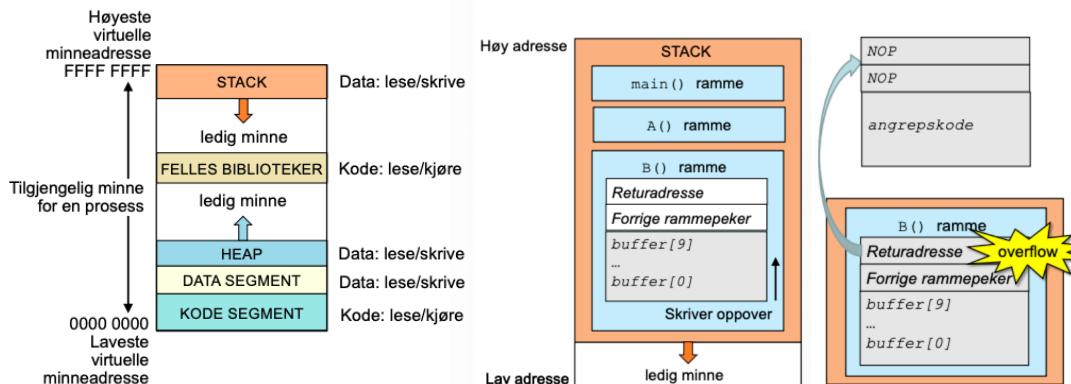
- Styrke systemsikkerhet
 - Fjern feil i OS
 - Sikkerhetoppdateringer
 - Sikkerhetsfunksjoner
 - Privilegienivåer
- Monitorering
 - Brannmur
 - Antivirus
- Virutualisering
- Tilltrodd beregning
 - Sikker oppstart med UEFI (Erstatter BIOS)
- CVE, common vulnerability & exposures
- CVSS, common vulnerability scoring system

Kjørbare filer

- Består av bytes
 - Binær fil
- Kjøres av CPU
- Oppretter en prosess
 - Allokerer minne
 - Laster nødvendig info til minnet
- Kjører instruksjoner
- Hver prosess har allokkert virtuelt minne
- Virtuelt minne blir oversatt til fysisk minne av OS
- Sørger for at prosesser har sitt eget fysiske adresseområde

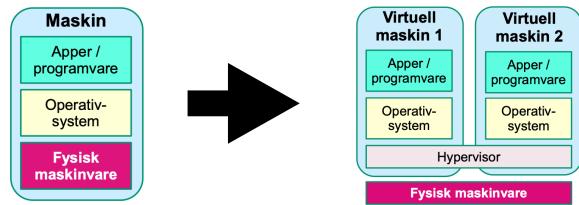
Buffer overflow

- Overskriver minnet
- Injiserer og kjører egen kode på samme privilegienivå
- Mottiltak:
 - NO EXECUTE
 - Stack Canaries
 - ASLR, Adress Space Layout Randomization
 - Skriv bedre kode
 - Sikre programmeringsspråk

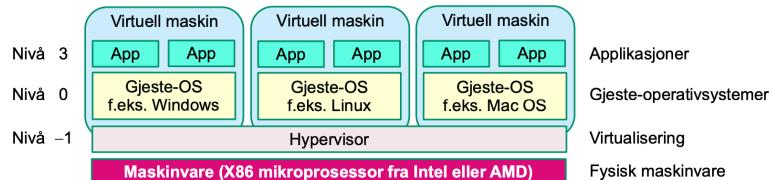


Virutualisering

- Adskille hardware (firmware) fra OS og apper.



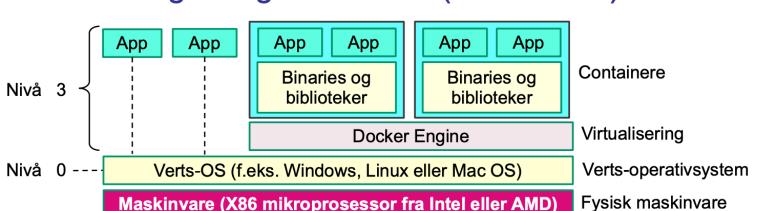
Type 1 virtualisering (native)



Type 2 virtualisering (vertsbasert)

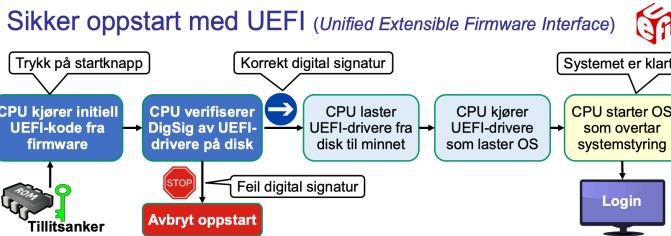


Docker Engine og containere (vertsbasert)



Tiltrodd beregning

- Trusted computing
- Sikkerhet forankret i maskinvare
 - Robust mot flere trusler enn programvare
- Sikker oppstart med UEFI
- TPM, Trusted Platform module
 - Innebygget kompressor
 - 3 funksjoner
 - Secure boot
 - Remote Attention (3rd party attention of safe state)
 - Disk kryptering
- TEE, trusted execution environment
 - Maskinvareteknologi
 - Beskytter data og beregninger i mikroprosessoren (INTEL SGX)
- Fysisk innkapsling
 - Manipuleringsbestandig
 - Sletter sensitiv informasjon hvis detektert angrep
- UEFI, Unified extensible firmware interface
 - Erstatter BIOS
 - Digitalt signert oppstart (Leverandør)
 - Platform key verifiseres



Sidekanal

- En utilsiktet kanal utenfor grensesnittet

Skjult kanal

- En tiltenkt mekanisme
 - Ikke for kommunikasjon
 - Kan misbrukes

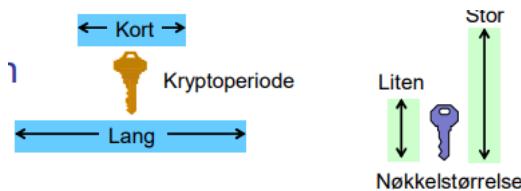
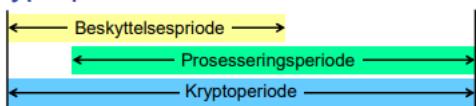
Nøkkelhåndtering

- Kryptonøkler
- Sikrer generering, lagring, distribusjon og destruering

Krypteringsperioder

- **Kryptoperiode**
 - Tidsperiode for godkjent bruk av en nøkkel
- **Beskyttelsesperiode**
 - Tidsperiode hvor data må beskyttes, krypteres
- **Prosesseringsperiode**
 - Tidsperiode hvor data må kunne dekrypteres
 - Alle perioder bestemmes iht. sensitivitet på data.
 - Bit-size iht. regnekapasitet

Kryptoperioder

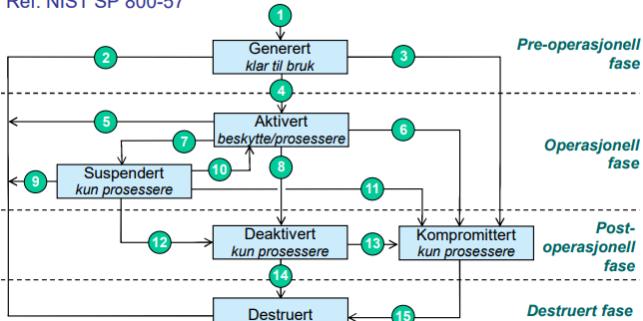


Nøkkelsegenerering

- Mest sensitive steget
- Tilfeldig valgte nøkler fra hele nøkkelsrommet
- Overføres aldri "klart"
- Konfidensialitetsbeskyttet
- Destruere nøkler totalt
- Destruering av masternøkkel
 - Fører til destruering av alle underordnede nøkler

Nøkkeltilstand, transisjoner og faser

Ref: NIST SP 800-57



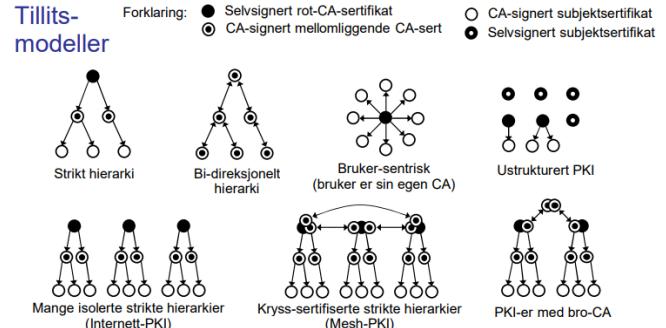
PKI, Public-Key Infrastructure

- Består av
 - Policy
 - Teknologier
 - Prosedyrer
 - Tillitsmodell
- PKI distribueres med sertifikater
 - Signeres digitalt, garanterer autentisitet
- Datarecord, hashes
- Haset record, signeres (digisig)

Tillitsmodeller og mellomledd

- Ulike CA:
 - Rot CA (Certification of Authenticity)
 - Mellom CA
 - Bruker
- Ulike modeller med ulik struktur.
- Modell bestemt basert på strikthet og grad av dependency på RotCA.
- Større organisasjoner har ofte større dependency.

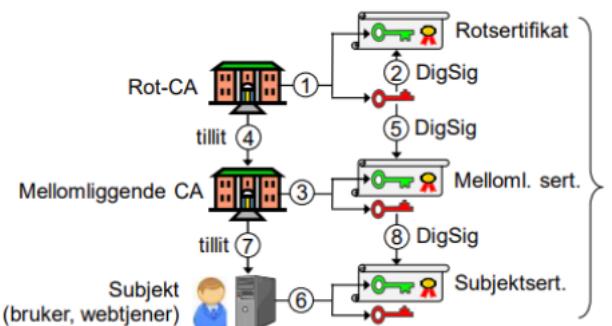
Tillitsmodeller



Generere offentlig nøkkelsertifikat:

PKI og internett

- HTTPS
- Lagret certifikater i nettleser



- OBS! Falske CA kan lagres for å gi inntrykk av en autentisk tjeneste.

Angrepsvektorer

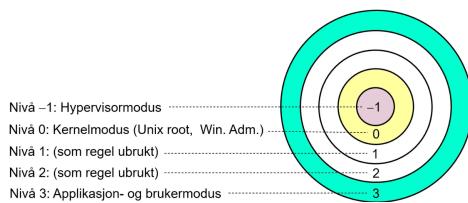
- Skadevare
 - Samlebegrep for programkode som utfører handlinger uten tillatelse
- Vektor
 - Måte/vei å overføre skadevare

Typer angrep:

- Drive-by
 - Infisert side, nedlasting av JS eller XSS
- Phishing
 - Masse, spear, whale og klone
 - Kultur som beste forsvar
- Deepfake
 - Ai-generert
- Sosial Manipulering
 - Folk er snille, spør
- Innsideangrep
 - Utro tjener
- Falske Nettsider
- Direkte nettverksangrep
 - Automatisk spredning av skadevare (dataorm)
- SQL Injeksjon
 - Databasetilgang
- Command Injection
 - Terminal command injection
- Man in the middle (MitM)
 - Lytter på trafikk, og genererer trafikk
- Downgradeangrep
 - Lurer maskinvare til å bruke dårligere kryptering
- Leveransekjedeangrep
 - Angrep på en partner/leverandør og får tilgang gjennom dem.

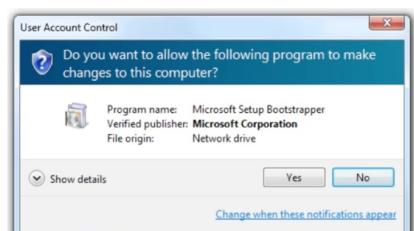
Typer skadevare

- Virus, trojaner, løsepengenvirus, dataorm, spyware, exploit, bott-program, bakdør, JS, makrovirus, logisk bombe.



Privilegienivå og skadevare

- Målet er å oppnå høyeste privilegienivå
- Skadevare kjører på samme nivå som bruker initialiserer den på
- Privilege escalation angrep
 - ROOTKIT, Zero-days (ukjente sårbarheter)



Pentesting

- Utpøye og avdekke sikkerhetshull
- HVIT/GRÅ/SVART
 - Bokstesting, ulik grad av info
- Motivasjon skiller hackere og pentestere
- Faser:
 - Planlegge
 - Recogniser
 - Innledende tilgang
 - Utvide tilgang
 - Gevinst
 - Rapport
- Verktøy:
 - Planlegg
 - Recog: OSINT
 - IP-adresse
 - Få tilgang
 - Boot-tilgang
 - Phishing
 - Utvide tilgang
 - Bli kjent med system
 - Let etter muligheter
 - Direkte angrep
 - Passordspraying
 - /etc/sudo
 - /usr/bin/cat (leseverktøy)
 - Passordknekking
 - Lateral Movement
 - Prøv og utnytt sårbarheter
 - Fuzzing
 - Gevinst
 - Rapport

Til eksamen:

- Forskjellige verktøy for pentesting
- Sett deg inn i John the ripper, shadow filer (fra oblig)
- Eks fra eksamen:
- Lagre passordhashene:
 - sudo cat /etc/shadow > /tmp/shadow
 - sudo cat /etc/passwd > /tmp/passwd
- Klargjør fil for John the Ripper:
 - unshadow /tmp/passwd /tmp/shadow > knekkes.txt
- Cracke passordene:
 - john knekkes.txt
- Med root-tilgang kan du også lese andre filer, som passord og SSH-nøkler, for eksempel:
 - sudo cat /home/bruker/.ssh/id_rsa
- **Regler** i John the Ripper er tilpasninger som endrer ordlistens passordkombinasjoner for å teste flere variasjoner, som store og små bokstaver eller tallkombinasjoner. De gjør cracking mer effektivt ved å prøve vanlige passordmønstre og variasjoner.

Brukerautentisering

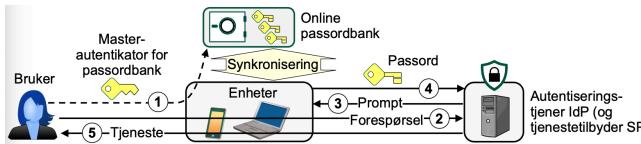
- Noe du vet
 - Passord
- Lagring av passord i system:
 - Linux: etc/shadow
 - Windows: SAM DB Security Account Manager
 - Nettverksmiljøer: AD/LDAP Active Directory, Lightweight Directory access control
- Nivåer av passordlagring
 - Klartekst, svak sikkerhet
 - Hashed, moderat sikkerhet
 - Salted, god sikkerhet
- Salting
 - Tilføy tilfeldig data (tall) til passord før kryptering
 - Gir forskjellig hash for samme passord

Passordangrep

- Brute force
- Intelligent søk

Passordbanker (PW, Managers)

- Innebygd i OS
- Innebygd i nettleser
- Tredjeparts PW manager
- Hvem stoler du på til å holde dine data?

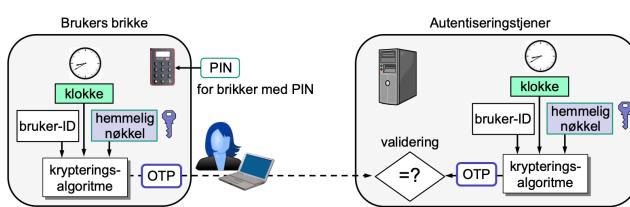


Noe du har: Autentiseringsenheter

- Kort, brikke, sekundære kanaler, online enheter
 - f.eks eID, FIDO...

One time-passord innlogging

- Klokkeavhengig
- Tidspunkt del av algoritme



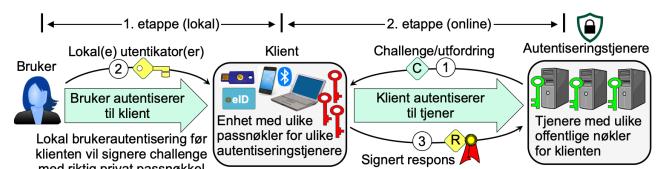
Phishingresistent autentisering

- Klient har en autentifikator
- Autentifikator sitter på private nøkler
- Nøklene har referanse til domenenavn
 - Skal samsvar med domenenavn man logger på
- ID-spoofing: "Falske" domener får tak i, eller utnytter autentifikatorer.
- Ikke-phishing resistente autentiseringer krever at bruker forstår domenenavn



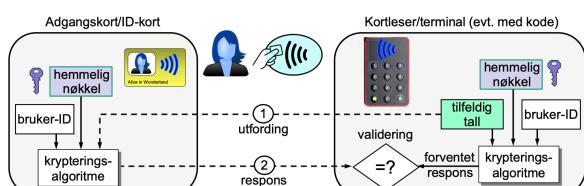
Autentisering med FIDO/WebAuthn

- FIDO og WebAuthn er resistente.
- Klient har en autentiseringstjener
- Gjennomfører autentisering i to etapper
 - Lokal etappe: Må godkjennes før online.
 - Inneholder domenenavn til autentiseringstjenesten
 - Online etappe: info fra tjener sjekkes mot lokal autentisering.
- Autentisering gjøres med passkeys
 - Kryptografisk privat nøkkel
 - Unik passkey for ulike autentiseringstjenere.
- Fordeler:
 - Finner ikke passkey for falske nettsider
- Utfordringer:
 - Komplisert å synkronisere til ny enhet
 - F.eks BANKID på mobil med ny telefon
 - Basert på lagring i skyen
 - Krever til syvende og sist tradisjonell autentisering med passord/2FA



Adgangskort, ID-kort og pass

- Kontaktløse kort RFID (ID-kort)
- Strøm genereres av magnetfelt
- Challenge fra enhet den sjekkes imot.



NFC (Near field communication)

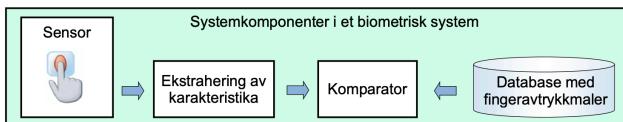
- Ofte brukt på mobil, samme prinsipp.

Sekundære kanaler

- SMS, App, Epost, SIM
 - Noen sekundære kanaler er sikrere enn andre
 - Kan være nødvendig med sekundær kanal for autentisering.

Noe du er: Biometri

- Fingeravtrykk, ansiktsgjenkjenning, retina/iris scan, håndgeometri, signatur, stemme/tale, dynamikk (handlingsmønstre) f.eks captcha basert på musepekeradferd)
 - Krav:
 - Universalitet
 - Særpreg
 - Permanens
 - Målbarhet
 - Nøyaktighet
 - Ytelse
 - Aksept
 - Beskyttelse mot forgjengning



PAD - Presentation attach detection

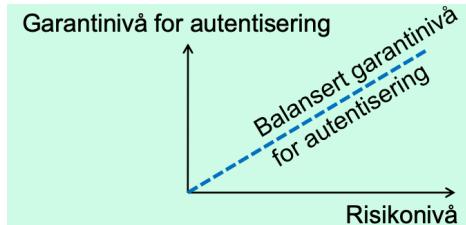
- Presenterer falsk, eller etterliknet biometri for å prøve å få tilgang. F.eks bilde istedenfor ansikt
 - 2FA, MFA kombineres ofte for å sikre biometri data.



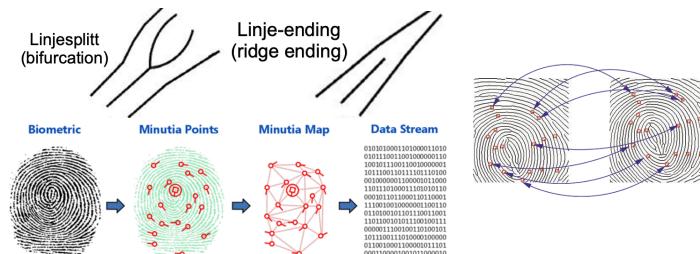
Falsk finger Falsk ansikt Deepfake lyd/bilde/video

Kontinuerlig autentisering

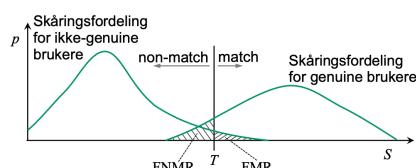
- Etter pålogging
 - Basert på maskinlæring
 - Kan også være signatursbasert
 - Handler om å detektere avvik i adferd
 - Oppnå "balansert garantinivå"
 - Et balansert nivå indikerer robusthet.



- Registrering av biometri:
 - **Identifikasjon: 1 : N**
Sammenlikne med mange
 - **Autentisering: 1 : 1**
Bekrefte en enkelt prøve



- Sammenlikning:
 - Sammenlikning, score: **S**
 - Terskel, verdi: **T**
 - **Match** = $(S \geq T)$
 - **Non-match** = $(S < T)$
 - **FMR**: False match rate
 - **FNMR**: False non-match rate
 - Dersom **FMR** = **FNMR** == **EER**
 - Equal error rate



E-forvaltning

- Bruk av digitale verktøy for å effektivisere offentlig administrasjon og tjenester
- Har til formål å:
 - Beskytte personopplysninger
 - Sikre personopplysninger
 - KIT + P
 - Styrke tillit til data
- Garantinivåer (LoA, Level of Assurance)
 - Low, medium high
- Kravkategorier i e-forvaltning
 - Krav til ID og korrekt registrering
 - Krav til klargjøring og håndtering av autentikator
 - Krav til autentiseringsmetoder
 - Krav til sertifisering av autentiseringstjener (IdP), portal og juridiske avtaler mellom interessenter.
- eIDAS: EU sin forskrift
 - 3 LoA nivåer (Low, medium, high)

Veileder/standard for autentisering	Garantinivå for autentisering		
SP 800-63-4 Digital Identity Guidelines NIST, USA 2025	Assurance Level 1	Assurance Level 2	Assurance Level 3
Assurance levels for electronic identification means eIDAS 2.0, EU 2024	Low	Substantial	High
Veileder for identifikasjon og sporbarhet DigDir 2022 (basert på eIDAS 1.0, 2018)	LAVT	BETYDELIG	HØYT
IS 29115 Entity authentication assurance framework ISO/IEC 2013	Low (1)	Medium (2)	High (3)
			Very High (4)

Identitet

- Består av attributter
- Entitet -> Identitet -> Digital Identitet
 - En digital identitet har navn, og attributt(er)
 - Disse kan være:
 - Entydig/tvetydige
 - Kortvarig/permanent
 - Selvdefinert eller definert av autoritet
 - Man velger selv hvordan en identitet skal identifiseres innad sitt system.
- identifikator: Krever et entydig unikt "navn"

Identitetshåndtering

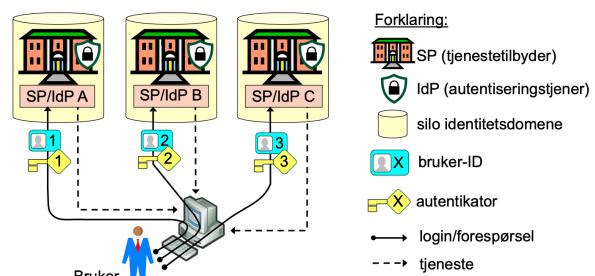
- Opprettelse, registrering
- Identitet betyr "samme som forrige gang"
- Autentisering -> gir mulighet for autorisering
- Pre-autentisering -> ID basert på tidligere ID
- Ny autentisering -> Ny id f.eks ved fødsel

ID Domener

- Navnerom med unike navn
- 1 identitet (en bruker) kan holde på flere identiteter (roller) innad et domene.

Silodomene(r)

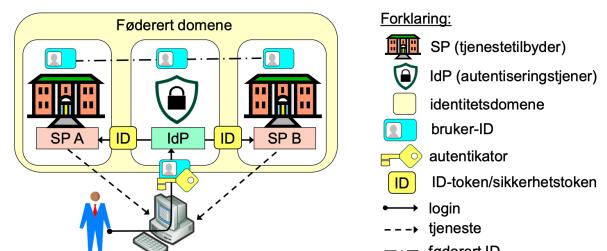
- SP = Service provider
 - IdP = Autentiseringstjener
- Se figur
- Hver SP har egen IdP, resulterer i mange innlogginger N:N
 - Fordeler
 - Lett å sette opp
 - Godt grunnlag for personvern (adskilte tjenester)
 - Ulemper
 - Identitetsoverlast
 - "Flere innlogginger"
 - Lav aksept for mange innlogginger, og vanskelig å samle inn brukerdata



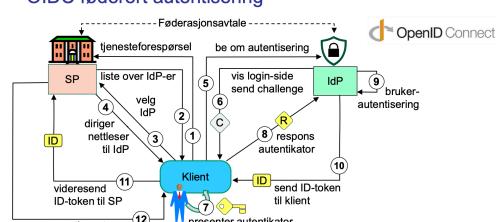
Fødererte domener

- SP = Service provider
 - IdP = Autentiseringstjener
- Se figur
- Hver SP bruker felles IdP, resulterer i én innlogging for mange tjenester 1:N
 - f.eks google, apple, Microsoft etc...
 - Fordeler
 - Mer brukervennlig
 - SP fokuserer på tjeneste, ikke idP
 - IdP kan enklere samle brukerdata
 - Skalbart
 - Ulemper
 - Teknisk og juridisk komplisert (å samkjøre)
 - Tillitskrav mellom aktører
 - Personversutsfordring

ID-føderering use-case



OIDC føderert autentisering



Standarder

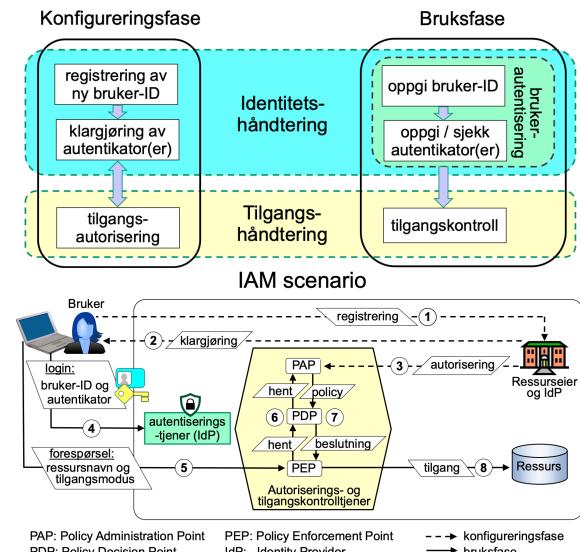
- **OAuth:** Brukes til å gi tredjepartsapper tilgang til en brukers data uten å dele passord. Det handler om **autorisasjon**.
 - Brukes for føderasjonsavtaler mot SPer.
- **OIDC (OpenID Connect):** Bygger på OAuth 2.0 og legger til **autentisering**. Dette betyr at det også bekrefter identiteten til brukeren, så det er ideelt for SSO (én innlogging for flere apper).
 - FEIDE, ID-Porten, HelselD
- **SAML (Security Assertion Markup Language):** Brukes hovedsakelig i bedrifter for SSO mellom interne systemer. Det håndterer både **autentisering og autorisasjon** og bruker XML for å utveksle data.
- OAuth = autorisasjon, OIDC = autentisering + autorisasjon for webapper, og SAML = autentisering + autorisasjon for bedriftssystemer.
- Distribuert tilgangskontroll med OAuth
 - I moderne applikasjoner er ressurs-eier og ressurs-tjener ofte separate fysiske, logiske og juridiske entiteter
 - Tilgangskontroll gjøres av ulike entiteter, avhengig av arkitektur
 - OAuth (Open Authorization) er en standard for å definere ulike arkitekturen for tilgangssautorisering og tilgangskontroll
 - OAuth omfatter, og brukes sammen med OIDC (OpenIDConnect)

Distribuert tilgangskontroll på internet med OAuth



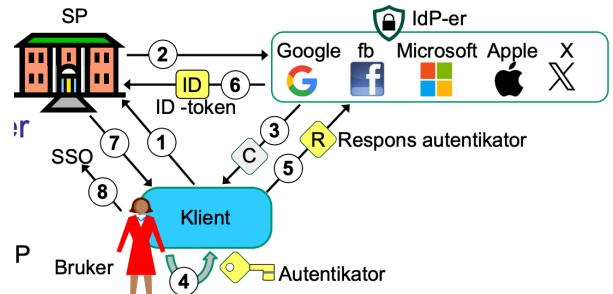
IAM Autorisering til venstre, autentisering til høyre

- Autorisering er å gi tilganger
- Autentisering er å bekrefte om credentials skal gis tilgang
 - Identitetshåndtering -> tilgangshåndtering



Sentralisering og distribuering

- **Sentralisert navnerom:** Ett system for alle brukernavn og ressurser.
- **Distribuert navnerom:** Flere systemer håndterer brukernavnene, ofte delt opp.
- **Sentralisert autentisering:** Ett sted for pålogging (som SSO for alle systemer).

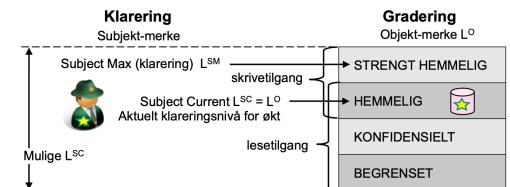


- **Distribuert autentisering:** Flere steder for pålogging, hver tjeneste kan ha sitt system.

Kategori av foderering	Sentralisert navnerom	Distribuert navnerom
Sentralisert autentisering	Tysk eID AADHAAR	FEIDE eduroam
Distribuert autentisering	ID-porten altinn HelseID	Google fb Microsoft X Apple Europisk eID

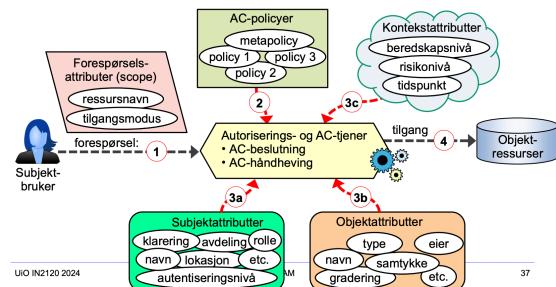
Tilgangskontroll

- **DAC (Discretionary Access Control):** Eieren av ressursen styrer tilgangen, f.eks. hvem som kan lese eller skrive en fil.
- **MAC (Mandatory Access Control):** Tilgang styres av sikkerhetsnivåer bestemt av systemet, ikke eieren. Brukes ofte i høysikkerhetssystemer.
Bell-LaPadula (MAC-modell) Klareringsnivå for økt
• For praktisk å kunne redigere dokumenter kan en bruker (subjekt) velge et aktuelt klareringsnivå for en spesifik økt på samme eller lavere nivå enn sitt egentlige klareringsnivå. Brukeren kan alltid redigere dokumenter med samme gradering som sitt aktuelle klareringsnivå.



- **RBAC (Role-Based Access Control):** Tilgang gis basert på brukerens rolle, f.eks. "admin"
- **ABAC (Attribute-Based Access Control):** Tilgang baseres på flere attributter, som tid, plassering eller brukerens egenskaper.

ABAC – Attribute Based Access Control

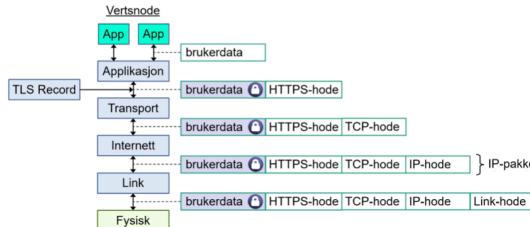


Nettverkssikkerhet

- Løkmodell til grunn
- FLITA: Lag i internettstakken

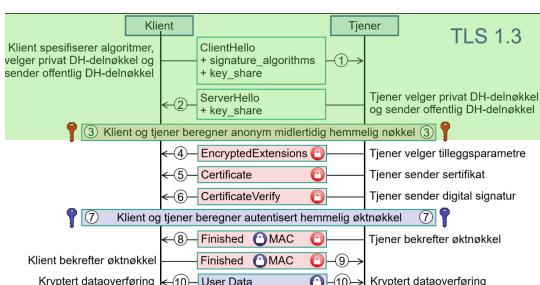
TLS

- TLS går inn under applikasjonslaget og krypterer brukerdata.
- Handshake protokoll



TLS 1.3

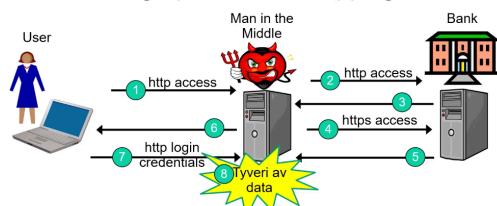
- **Nøkkelutveksling:** Benytter Diffie-Hellman for sikker nøkkelutveksling.
- **Øktnøkkel:** Genererer en hemmelig kryptert øktnøkkel etter én meldingsrunde, noe som reduserer forsinkelser.
- **Fremoverhemmelighet:** Øktnøkkler sikrer fremoverhemmelighet; selv om en langsigkt krytonøkkel kompromitteres, vil tidligere øktnøkkler fortsatt være sikre.



TLS Stripping

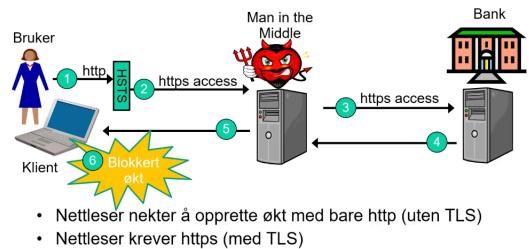
- Et Man-in-the-Middle (MitM)-angrep der angriperen nedgraderer HTTPS-trafikk til HTTP mot bruker for å kunne lytte.

Angrep med TLS-stripping



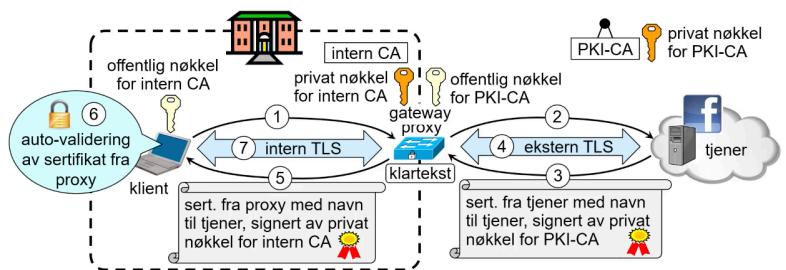
- **Forsvar (HSTS):** HTTP Strict Transport Security (HSTS) hindrer TLS-stripping ved å:
 - Kreve HTTPS for alle tilkoblinger.
 - Terminere tilkoblingen hvis HTTPS ikke detekteres.
 - Være standard i Chrome-baserte nettlesere, men krever at brukeren besøker HTTPS-siden én gang for å aktivere.

- Nettleseren lagrer "https://" i policy for fremtidige besøk.



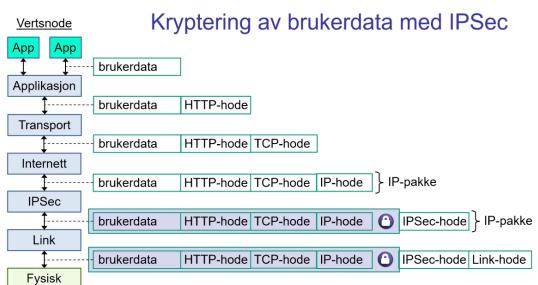
TLS Inspeksjon

- Verktøy som ofte brukes av organisasjoner for å inspisere HTTPS-trafikk fra ansatte (kan anses som overvåking).
- **Metode:** En proxy/gateway utgir seg som den eksterne tjeneren og dekrypterer trafikken.
- **Validering:** Proxy-serverens sertifikat valideres automatisk slik at maskinen oppfatter tilkoblingen som sikker (TLS)



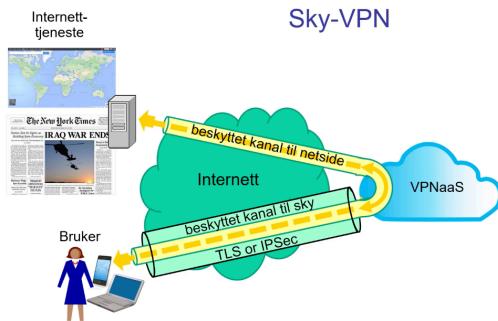
IPsec

- IPsec er et OS-basert verktøy for sikker dataoverføring over IP-nettverk, ofte brukt i VPN-er for å lage sikre tunneler.
- Går inn mellom IP- og link-laget i internettstakken
- Funksjon: Lager en IPsec header på hele pakken før link-laget:
 - **Kryptering:** Beskytter dataene så de holdes private.
 - **Autentisering:** Bekrefter hvem som sender dataene.
 - **Integritet:** Sikrer at dataene ikke endres underveis.
 - **Transport:** Krypterer kun dataene, ofte brukt mellom to enheter.
 - **Tunnel:** Krypterer hele IP-pakken, ofte brukt i VPN.



VPN (Virtual Private Network)

- Oppretter en beskyttet kanal for sikker dataoverføring mellom en enhet og et nettverk.
- VPN har blitt viktig i **BYOD-kulturen** (Bring Your Own Device), der ansatte bruker egne enheter som kan være oppdaterte og dermed gi sikkerhetshull.
- Hvem ser hva ved bruk av VPN?
 - **Bruker:** Ser alt som normalt.
 - **Internetleverandør (ISP):**
 - Ser tilkoblingen mellom bruker og VPN-server.
 - Ser trafikken som går til VPN-serveren, men ikke det videre innholdet.
 - **Nettside:**
 - Ser IP-adressen og trafikken som kommer fra VPN-serveren, ikke brukerens faktiske IP-adresse.



TOR-Løkruting

- En slags VPN som "hopper" og krypterer trafikk (hvert hopp) over flere maskiner (ofte 3).
- Godt anonymiseringsverktøy
- Utsetter dog egen IP for routing.
 - Kan medføre risiko ved "nefarious" formål.

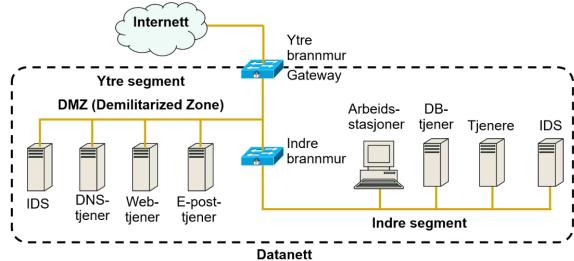
Standardporter for kjente tjenester (EKSAMEN!)

- **HTTP (80):** Webtrafikk.
- **HTTPS (443):** Kryptert HTTP-trafikk.
- **SSH (22):** Kryptert fjernpålogging.
- **Telnet (23):** Tidligere fjernpålogging (ukryptert) – kun "trygg" med TLS/VPN.
- **RDP (3389):** Remote Desktop Protocol for Windows.
- **FTP (21):** Filoverføringsprotokoll (ukryptert).
- **DNS (53):** Oversetter domenenavn til IP-adresser.

Brannmur

- Et sjekkpunkt som beskytter et nettverk mot andre nettverk, ved å kontrollere hvilken trafikk som får passere.
- **Løk-prinsipp:** Plasser brannmurer naturlig der det trengs – beskytt DMZ fra internett, og det interne nettverket fra DMZ.
- **Segmentering:** Bruk flere brannmurer for å dele nettverket i segmenter (subnett) med like funksjoner, som gir bedre sikkerhetskontroll.

Enkel datanettarkitektur med brannmurer



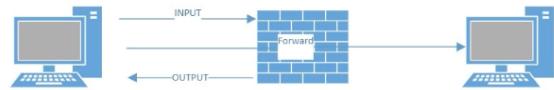
Typer brannmurer

Tilstandsløse brannmurer

- Enkleste typen brannmur som inspiserer pakkehoder på transport og internett-laget, og basert på dette bestemmer om pakke skal godtas eller avvises.
- Bruker IP-adresse, portnummer, type transportprotokoll
- Kallas ofte Pakkefilter
- Må konfigureres med IP Tables.

IP Tables

- En kommandolinjebasert brannmur i Linux som administrerer nettverkspakker basert på IP, port og protokoll. Konfigureres med regler for å kontrollere innkommende og utgående trafikk.



iptables - Viktige kommandoer og flagg

- **A <liste>:** Angir kjeden (liste) hvor regelen legges til:

- **OUTPUT:** Regelen gjelder utgående trafikk fra verten.
- **INPUT:** Regelen gjelder innkommende trafikk til verten.
- **FORWARD:** Regelen gjelder trafikk som videresendes gjennom verten.
- **-s <IP-adresse>:** Spesifiserer IP-adressen til avsenderen. Dette kan være en spesifik IP eller et nettverk (f.eks. 192.168.1.0/24).
- **-d <IP-adresse>:** Spesifiserer IP-adressen til mottakeren. På samme måte kan det være en spesifik IP eller et nettverk.

- **--sport <portnummer>:** Spesifiserer portnummeret til avsenderen. Brukes til å begrense regelen til spesifikke avsenderporter.

- **--dport <portnummer>:** Spesifiserer portnummeret til mottakeren. Brukes til å begrense regelen til spesifikke mottakerporter.

- **-p <proto>:** Spesifiserer protokollen som brukes (f.eks. tcp, udp eller icmp).

- **-j <result>:** Angir hva som skal skje med pakken når den møter regelen:

DROP: Pakken forkastes uten varsel.

ACCEPT: Pakken tillates og går videre.

Tilstandsbaserte brannmurer

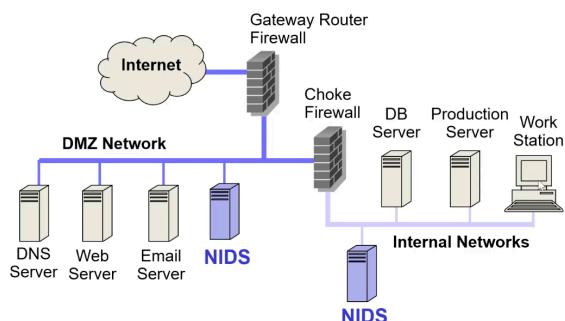
- Holder oversikt over tilstander i aktive økter mellom klient og server.
- **Fordel:** Kan opprette midlertidige regler for spesifikke økter, noe som gir fleksibilitet og høy ytelse.
- **Ulempe:** Krever minne for å spore øktene.

Applikasjonsbrannmur

- Inspiserer dataene i selve pakkene (ikke bare hoder) og støtter spesifikke applikasjonsprotokoller (f.eks. HTTP, FTP).
- **Bruk:** Filtrerer trafikk fra spesifikke applikasjoner og fungerer som proxy (kalt proxy- eller gateway-brannmur).
- **Next-Gen brannmur:** Høyytelses applikasjonsbrannmurer med avansert filtrering for moderne applikasjoner og trusler.

Intrusion Detection System (IDS)

- Et system designet for å detektere mistenkelig eller uønsket aktivitet som kan tyde på et sikkerhetsbrudd.



Typer IDS

HIDS (Host-Based Intrusion Detection System)

- Overvåker spesifikk aktivitet på et host-system.
- Filer, filendringer, og prosesser på vertsmaskinen.
- Gir detaljert innsikt på individuelle maskiner og kan identifisere kompromitterte filer eller prosesser.

NIDS (Network-Based Intrusion Detection System)

- Overvåker aktivitet på et nettverkssegment.
- Analyserer nettverkstrafikk for å identifisere mistenkelige mønstre eller uønsket aktivitet.
- Kan være sensitivt med tanke på personvern siden det monitorerer all trafikk på nettverket.

Metoder for deteksjon

Signaturbasert IDS

- Oppdager kjente trusler basert på tidligere identifiserte signaturer.
- **SNORT** er et populært signaturbasert IDS som kan identifisere trusler gjennom kjente "signaturer."

- Kan bare oppdage kjente trusler med eksisterende signaturer, og er mindre effektivt mot nye angrep.

Anomalibasert IDS

- Oppdager avvik fra en normal adferdsmonster.
- Bruker ofte maskinlæring for å definere hva som er "normalt" og detektere avvikende aktivitet.
- Kan oppdage nye trusler som ikke har eksisterende signaturer.
- Kan føre til falske positive (feilalarmer) og krever kontinuerlig overvåkning etter innledende autentisering.
- NIDS basert på denne metoden varsler ofte ved en "spike" i uventet aktivitet.

IPS, Automatisk inntrengingsdeteksjon

- Automatisk innlegg av regler
- Blokkering av tjenester
- Ressurskrevende
 - Utsatt for DoS/DDoS

Honeypot

- Falskt, attraktivt mål, gjerne upatchet
- All trafikk er emulert (falsk)
- Overvåk alt til og fra
 - Se og lære av hva angriper gjør på maskinen

SOC (Security Operations Center)

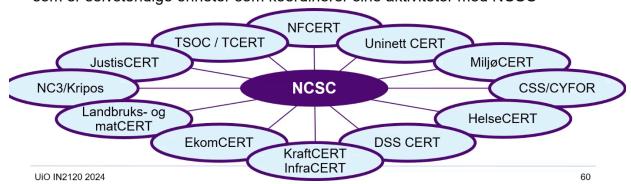
- Et sentralisert senter som overvåker og beskytter en organisasjons sikkerhet.
- Kontinuerlig trusselovervåkning, hendelsesrespons, og analyse.

Responsteamtyper

- **CERT** (Computer Emergency Response Team): Håndterer nødrespons ved cybertrusler.
- **CIRT** (Cyber Incident Response Team): Fokuserer på å reagere på sikkerhetshendelser.
- **CSIRT** (Computer Security Incident Response Team): Ekspertteam som analyserer og svarer på sikkerhetshendelser.
- Disse teamene har overlappende roller, men har hver sine spesifikke fokusområder.

NCSC og sektorvise responsmiljøer

- NCSC (Nasjonalt cybersikkerhetscenter), som er en del av NSM, er nasjonal koordinerende enhet for sikkerhetshendelser med hensyn til deteksjon, hendelsesrespons og koordinering.
 - Inneholder NorCERT som er den nasjonale CERT
- I tillegg til NCSC er det opprettet en rekke sektorvise responsmiljøer (SRM), som er selvstendige enheter som koordinerer sine aktiviteter med NCSC



Sikkerhetskultur

- Bevissthet og adferd rundt digital sikkerhet, med vekt på personlig integritet og forsvar mot sosial manipulering. Målet er å forhindre innsidetrusler og sikre at ansatte forstår og etterlever sikkerhetsnormer.
- Definisjoner:
 - **ISACA:** Sikkerhetskultur er kunnskap, holdninger og verdier om sikkerhet, manifestert i menneskers adferd.
 - **NSM:** Sikkerhetskultur er summen av ansattes kunnskap, motivasjon og atferd for virksomhetens totale sikkerhet.

Dimensjoner: HAKKONA

- Holdninger, Atferd, Kognisjon, Kommunikasjon, Overholdelse, Normer, Ansvar

Utvikling av sikkerhetskultur:

- Ledelse som forbilde, forståelse av nåværende tilstand, målbare forbedringspunkter, og bruk av positive tiltak for å forbedre bevissthet og adferd.

Personlig integritet

- Fokus på ansatte, ledelse og andre aktører med tilgangsprivilegier for å minimere

Innsidetrusselen:

- **Styrking av integritet:** Bevissthetstrening, policy-påminnelser, empowerment, og støtte i spesielle situasjoner.
- **Ansatte som slutter:** Klare prosedyrer for å fjerne tilgangsrettigheter ved avslutning, enten gjennom avtalt offboarding eller umiddelbar sletting.

Ledelsens rolle

- Viktig for å håndtere innsidetrusselen ved å være oppmerksom på adferdsendringer, opptre rettferdig under nedbemannning, og sørge for god kommunikasjon med ansatte.

Sosial manipulering

- Sosial manipulering utnytter mennesker som det svakeste ledd. Dette kan skje via teknologiske midler (e-post, SMS) eller i fysisk møte.
- Mål: å få offeret til å utføre handlinger som gagner angriperen.
- **Phishing:** Mass-, Spear-, Whale-, Clone Phishing.
- **NLP:** Bruk av kroppsspråk og tonefall for å påvirke underbevisstheten til offeret.

Taktikker

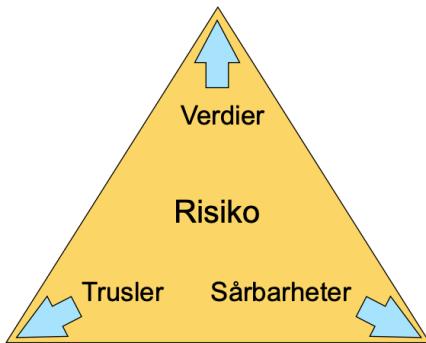
- **Bygge tillit:** Redusere skepsis og skape tilgang.
- **Indusere emosjoner:** Få offeret til å handle impulsivt.

- **Informasjonsoverlast:** Overvelde med informasjon for å fremprovosere feil beslutning.
- **Gjenytelse:** Skape en følelse av forpliktelse.
- **Autoritet:** Late som om man er i en maktposisjon for å påvirke handlinger.

Riskostyring

Typer risiko:

- **Kreditrisiko:** Risiko for at låntaker ikke betaler tilbake.
- **Markedsrisiko:** Risiko fra endringer i markedspriser.
- **Systemisk risiko:** Risiko for markedskollaps.
- **Operasjonell risiko:** Risiko fra feil i drift, system eller prosess.



ISO-standarder:

- **ISO 31000:** Definerer risiko som effekten av uvissitet på måloppnåelse; risiko omfatter både positive og negative effekter. Ofte uttrykt som sannsynligheten for en hendelse og dens konsekvens.
- **ISO 27005 (Informasjonssikkerhetsrisiko):** Risikoen for at en trussel utnytter sårbarheter i verdier, og dermed skader organisasjonen.
- **Riskomodell (NSM):** Risiko øker med verdi, trusselnivå og alvorlighetsgrad av sårbarheter.

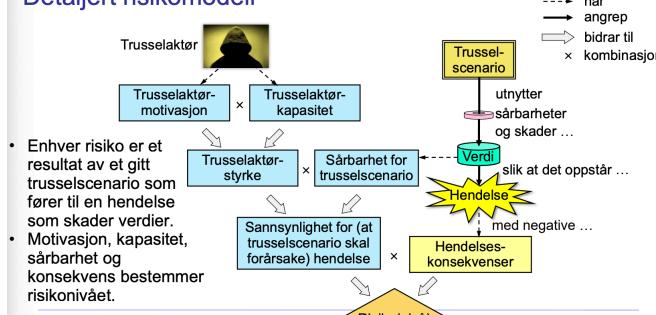
Trusler

- **Trusselscenario:** En sekvens av handlinger eller hendelser, utløst av en trusselaktør, som kan skade verdier dersom sårbarheter finnes.
- **Trusselaktør:** En entitet (menneske, natur) som kan utløse trusselscenarier, med eller uten hensikt om skade.

Risiko og risikonivå

- **Risiko:** Kombinasjon av trussel, sårbarhet, verdi og potensiell hendelse som kan skade virksomhetens verdier og bryte med sikkerhetsmål (KIT+P).
- **Riskoidentifisering:** Kartlegger kombinasjoner av faktorer som kan utgjøre en trussel mot verdier.
- **Riskonivå:** Sannsynligheten for en hendelse multiplisert med konsekvensen (risikoeksponering), beregnes gjennom risikoanalyse.

Detaljert risikomodell



Standarder for Riskostyring

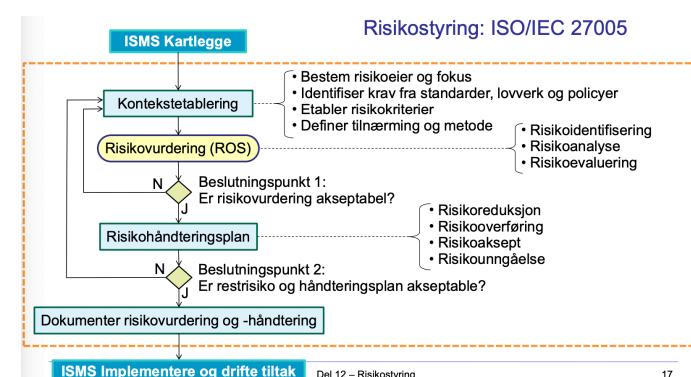
- **ISO 31000:** Generell riskostyring.
- **ISO/IEC 27005:** Riskostyring for informasjonssikkerhet.
- **NIST SP800-39 og SP800-30:** Styring og vurdering av informasjonssikkerhetsrisiko.
- **NS 5814, NS 5831, NS 5832:** Krav og retningslinjer for samfunnssikkerhet og beskyttelse mot tilsiktede hendelser.

Riskostyring

- Koordinerte aktiviteter for å identifisere, analysere og håndtere risikoer for å balansere tapspotensial med investering i sikkerhetstiltak.
- **Mål:** Gi oversikt over verdier, trusler, sårbarheter og eksisterende risikoer, foreslå tiltak, vurdere restrisiko, og støtte budsjetting og forsikringsvalg.
- **Metoder:** Kvalitativ, kvantitativ og relativ risikoanalyse med forhåndsdefinerte akseptkriterier.

Roller i risikostyring

- **Ledelse:** Overvåker og godkjenner budsjett.
- **Eiere:** Lager verdioversikt, setter sikkerhetsmål, vurderer konsekvenser.
- **Brukere og sikkerhetsekspert:** Identifiserer trusler og sårbarheter, vurderer sannsynligheter.
- **Riskoekspert:** Leder risikoanalyseprosessen.
- **Sikkerhetsekspert:** Anbefaler sikkerhetstiltak.



Beslutningspunkt 1: (modell over)

- Er risikovurderingen tilfredsstillende?
- Grunner for "Nei"?
 - Relativt dårlig spredning av risikonivåer
 - Spredning kan forbedres med reklaimbrering av sannsynlighet eller konsekvensnivå
 - For stor uvissitet rundt en eller flere høye risikoer
 - Uvissheten kan reduseres ved å gjøre mer grundig vurdering av riske risikoene

Beslutningspunkt 2: (modell over)

- Er håndteringsplanen akseptabel?
- Grunner for "Nei"?
 - For **høy** restrisiko

- Restrisiko kan senkes ved å implementere flere tiltak
 - Restrisiko defineres som **passe** ved å **heve** risikoterskel
- B. For **lav** restrisiko
- Restrisiko kan heves ved å redusere antall tiltak
 - Restrisiko defineres som **passe** ved å **senke** risikoterskel
- C. **Passe** restrisiko, men utilstrekkelig budsjett til å innføre foreslalte risikoreduserende tiltak
- Tilpass budsjett ved å øke budsjettet eller kutte tiltak.

tiltak mot en trussel. Identifikasjon skjer ofte ved bruk av sårbarhetsskannere og sjekklisten, som f.eks. **OWASP Top 10**.

- Trusler utløser potensielle sårbarheter. Eksempel: økt risiko på Karl Johan som følge av terrorhendelser i andre byer førte til installasjon av sperringer for å beskytte mot lignende hendelser.

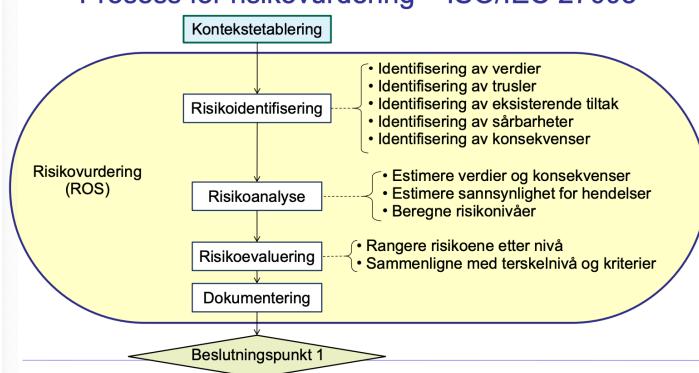
- Vurdering av konsekvenser

- En hendelse kan bryte sikkerhetsmålene for verdier (KIT+P), og konsekvensnivået estimeres for hver hendelsestype, basert på potensielle skader på ulike aspekter av verdiene.

- Redusert omsetning/profit, tap
- Svekket ytelse av tjeneste
- Brudd på juridisk etterlevelse, advokatutgifter, erstatning, bøter
- Skadet omdømme
- Kostnader ved håndtering og gjenopprettning
- Belastning på ansatte og brukere

Konsekvensaspektene vurderes som helhet. Den høyeste (mest alvorlige) konsekvens er tilnærmet lik helhetlig konsekvens.

Prosess for risikovurdering – ISO/IEC 27005



Riskovurdering

- Identifiser risiko

- Innebærer å finne en relevant kombinasjon av trussel, sårbarhet og hendelse som kan skade verdier.

- Kartlegging av verdier og ressurser

- Verdier omfatter et bredt spekter som driftsdata, persondata, systemdata, nettverk, applikasjoner og tjenester.
- Full oversikt er sjeldent mulig, men trusselmodellering peker ut de mest relevante verdiene.
- Ressurs-eier identifiserer disse verdiene og vurderer hvor viktige sikkerhetsmålingene (KIT+P) er for hver verdi, samt konsekvensene av eventuelle brudd.

- Trusselmodellering

- Trusselmodellering kartlegger angrepsscenarier gjennom identifisering, analyse og beskrivelse av relevante trusler.
- Viktige spørsmål er hva som kan skje, hvordan verdier kan skades, og hvem som er interessenter.

- Sårbarheter

- Sårbarheter representerer svakheter som kan utnyttes av trusselaktører for å angripe system- og informasjonsressurser.
- Sikkerhetssårbarheter må identifiseres og adresseres for å blokkere spesifikke trusler. En sårbarhet er fraværet av, eller en svakhet i,

Riskoanalyse

- Risikoanalyse vurderer risikonivået basert på to faktorer:

- **Sannsynlighet**: Hvor ofte hendelser kan inntrefte.

- **Konsekvens**: Potensiell skade ved hendelsen.

- Vurderingen kan gjøres på to måter:

- **Kvalitativt** (empirisk): Bruker analyser av sannsynlighet og konsekvens basert på erfaring.

- **Kvantitativt** (teoretisk): Matematisk beregning der sannsynlighet, P, uttrykkes som et tall i [0,1], og konsekvens, K, i pengeverdi. Risikonivå R beregnes som forventet tap pr år: $R = P \times K$.

Case: Hacking av website

- Risiko: hacking med tilgrising og ødelagt website
- Sannsynlighetsestimat
 - $P = 0,5$
- Konsekvensberegning
 - Tapt fortjeneste fordi websiden er nede, $k_1 = \text{NOK } 500\,000$
 - Tapt omdømme $k_2 = \text{NOK } 200\,000$
 - Kostnad med å rette opp websiden $k_3 = \text{NOK } 100\,000$
 - $K = k_1 + k_2 + k_3 = \text{NOK } 800\,000$
- Risikoberegning
 - $R = P \times K = 0,5 \times \text{NOK } 800\,000 = \text{NOK } 400\,000$
- Kan berette til NOK 400 000 for å håndtere risiko
 - hvis risikonivået reduseres til NOK 0

Riskoberegning

- **Kvantitativ** risikoberegning: Bruker $P \times K$ for et konkret estimat på forventet tap.

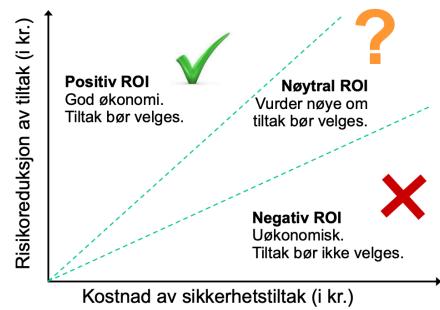
- **Kvalitativ** risikoberegning: En additiv tilnærming der $(S + K) / 2$ gir en relativ vurdering av alvorlighetsgraden.

- **Multiplikativ** risikoberegning: Kombinerer sannsynlighet og konsekvens med $P \times K = R$, noe som gir et mer kvantitatittiv perspektiv.

Økende sannsynlighet ↑

Kvalitativ sannsynlighetsskala

Sannsynlighet	Beskrivelse
(5) Svært høy	Det fins motiverete trusselaktører som med letthet kan nå sitt angrepsmål ved å gjennomføre det vurderte trusselscenarioet for denne risikoen. En hendelse er antagelig allerede i ferd med å skje, eller vil skje om kort tid.
(4) Høy	Motiverete trusselaktører vil med høy sannsynlighet nå sitt angrepsmål ved å gjennomføre det vurderte trusselscenarioet. En hendelse kan inntrefte noen ganger per måned.
(3) Betydelig	Trusselaktører har en betydelig mulighet til å nå sitt mål ved å bruke det vurderte trusselscenarioet. En hendelse kan inntrefte noen ganger per år.
(2) Lav	Trusselaktører har relativt liten mulighet til å nå sitt angrepsmål ved å bruke det vurderte trusselscenarioet. Det vil antagelig gå flere år mellom hver hendelse.
(1) Usannsynlig	Trusselaktører har svært liten mulighet til å nå sitt angrepsmål ved å bruke det vurderte trusselscenarioet. Det vil kanskje aldri skje en hendelse.



Kvalitativ konsekvensskala

Økende konsekvens ↓

Konsekvensnivå	Beskrivelse
(5) Svært alvorlig	Svært alvorlig skade på verdier, paralyserende tjenestavbrudd, svært stort økonomisk tap og mulig konkurs. Gjenopprettning krever langvarig arbeid med store ressurser. Eksterne funksjoner som avhenger av virksomheten kan falle bort i lang periode.
(4) Alvorlig	Alvorlig skade på verdier som kan medføre alvorlig tjenestevanbrudd og stort økonomisk tap. Det kreves store ressurser for å håndtere hendelsen. Funksjoner utenfor den berørte virksomheten kan bli negativt påvirket, men uten langvarige konsekvenser.
(3) Betydelig	Betydelig skade på verdier som kan medføre betydelig tjenestevanbrudd og betydelig økonomisk tap. Gjenopprettning og tjenestekontinuitet krever betydelig arbeid. Funksjoner utenfor virksomheten blir sannsynligvis lite påvirket.
(2) Liten	Relativt liten skade på verdier som kan true kvalitet av drift, og antagelig lite eller intet tjenestevanbrudd. Bare lite økonomisk tap. Håndteres greit med moderate ressurser.
(1) Ubetydelig	Ubetydelig skade på verdier, uten tjenestevanbrudd. Hendelser håndteres relativt lett som del av rutinemessig drift. Lite eller intet økonomisk tap.

Risikomatrise for kvalitativ risikoberegning

Risikomatrisen er en oppslagstabell med forhåndsdefinerte risikonivåer i hver celle

		Kvalitative konsekvensnivåer				
		(1) Ubetydelig	(2) Liten	(3) Betydelig	(4) Alvorlig	(5) Sv. alvorlig
Kvalitativ sannsynlighet	(5) Svært høy	(3) M	(4) S	(4) S	(5) SS	(5) SS
	(4) Høy	(2) L	(3) M	(4) S	(4) S	(5) SS
	(3) Betydelig	(2) L	(2) L	(3) M	(4) S	(4) S
	(2) Lav	(1) SL	(2) L	(2) L	(3) M	(3) M
	(1) Usannsynlig	(1) SL	(1) SL	(2) L	(2) L	(2) L

(5) SS: Svært stor risiko, må håndteres med høy prioritet
(4) S: Stor risiko, skal vanligvis håndteres
(2) L: Litен risiko, kan vanligvis aksepteres
(1) SL: Svært liten risiko, kan ignoreres

32

Antagelser i Risikoanalyse

- Verdier, trusler og sårbarheter identifiseres separat.
- Sannsynlighet og konsekvens estimeres hver for seg.
- Risikonivå beregnes før og etter nye tiltak, med og uten antagelse om tiltakseffektivitet.
- Kostnad for tiltak beregnes separat; nytte-kost vurderes ved ROI-estimat.

Risikhåndtering

- Sortér risiko etter alvorlighet og håndter dem basert på akseptnivå:
 - **Reduser:** Implementer sikkerhetstiltak.
 - **Del/overfør:** Eksempelvis outsourcing eller cyberforsikring.
 - **Behold:** Tolerer risikoen når kostnadene ved håndtering overstiger risikoen.
 - **Unngå:** Stopp aktiviteten som medfører risiko når ingen andre tiltak er tilstrekkelige.

ROI av sikkerhetstiltak

ROI beregnes som $(\text{Risikoreduksjon} - \text{Kostnad}) / \text{Kostnad}$.

For hver prioriterte risiko identifiseres tiltak for å redusere risiko, noe som etterlater en restrisiko. Det er opp til ledelsen å akseptere restrisikoen.

Mitigering av restrisiko

Planlegging og beredskap er nøklene til effektiv mitigering av restrisiko. Viktige tilnærminger inkluderer:

- **Incident Response Plan (IRP):** For håndtering av sikkerhetshendelser.
- **Disaster Recovery Plan (DRP):** For gjenopprettning etter større driftsavbrudd.
- **Business Continuity Plan (BCP):** For å sikre kontinuerlig drift under og etter kriser.

Evaluering og vedlikehold av risikostyringstiltak

- Risikostyring er en kontinuerlig prosess; tiltak for å redusere risiko må driftes, evalueres og justeres fortøpende for å sikre effektivitet og nøyaktig beregning av restrisiko.
- Prosesen opprettholdes så lenge organisasjonen har risikoeksponerte aktiviteter.

Positiv tilnærming til risiko

- Se risiko som en mulighet for vekst ved å:
 - Utforske alternative forretningsmodeller som gir økt fortjeneste uten tilsvarende økning i risiko.
 - Dele risiko og muligheter med andre aktører.
 - Være kjent med restrisikoen og forberedt på å håndtere og begrunne den om hendelser inntreffer.

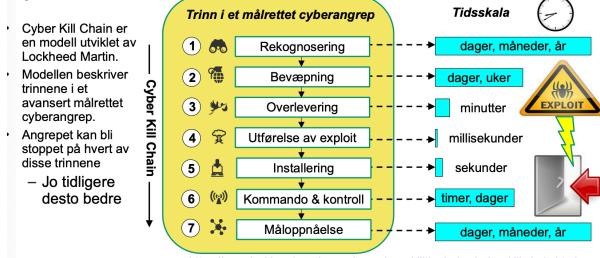
Helhetlig beslutningstaking om risiko



Cyberoperasjon

- Aktiviteter som innebærer angrep på eller forsvar av digitale infrastrukturer.
- Typer:
 - Offensive (cyberangrep, uautorisert tilgang)
 - Defensive (håndtering av datainnbrudd).
- Trusler:
 - Uautoriserte angrep fra kriminelle eller statlige aktører.
 - Sabotasje og datainnbrudd.
- Tiltak:
 - Offensive operasjoner: Avanserte cyberangrep.
 - Defensive operasjoner: Tiltak for å identifisere, håndtere og redusere konsekvensene av angrep.
- Avanserte Cyberoperasjoner - Eksempler
- **Statlige Angrep:** Angrep mot Helse Sørøst (2018), statsforvaltere (2018), Stortinget (2020/2021), Østre Toten (2021). Langvarig angrep, over flere steg.

Cyber Kill Chain



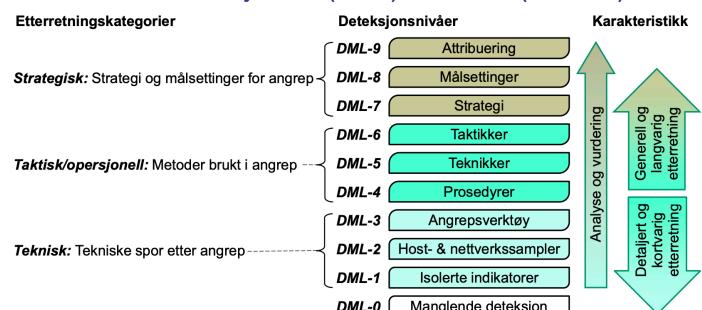
- **Cyber kill chain:** Beskriver trinnene i et målrettet cyberangrep; stopper angrepet tidlig for å redusere skade.
- CKC Trinn 1: Rekognosering
 - Identifisere sårbarheter i nettverket og samle informasjon om målet.
 - Eksempel: Firma velges for å hente informasjon; sårbarhet i tjeneste identifisert via skanning.
- CKC Trinn 2: Bevæpning
 - Lage skadeware (exploit) i et egnet format for levering til offeret.
 - Eksempel: Skadeware integreres i PDF-fil som skal imitere et anbud.
- CKC Trinn 3: Overlevering
 - Levere skadeware til målet (USB, phishing, webtjener).
 - Eksempel: Spear-phishing e-post med PDF vedlegg sendt til kontaktperson.
- CKC Trinn 4: Utførelse av exploit
 - Kjøring av exploit for å utnytte sårbarhet i målets system.
 - Eksempel: Kontaktperson åpner PDF-en, og exploit kjøres.

- CKC Trinn 5: Installerings
 - Installere skadeware og opprette tilgangspunkt (bakdør) for angriperen.
 - Eksempel: Bakdør åpnes, og angriper får ekstern tilgang.
- CKC Trinn 6: Kommando og Kontroll (K2)
 - Angriper får tilgang til nettverket, kan spre seg videre og skjule spor.
 - Eksempel: Angriper søker etter spesifik informasjon og skjuler sine spor.
- CKC Trinn 7: Måloppnåelse
 - Utføre det faktiske målet med angrepet, f.eks. datatyveri eller sabotasje.
 - Eksempel: Informasjon overføres skjult over lengre tid for å unngå deteksjon.

Detection Maturity Level (DML)

- Modell som beskriver modenhet for å detektere cyberangrep.
- Nivåer
 - Lav modenhet: Enkelt å detektere tekniske spor som IP-adresser og domener.
 - Høyere modenhet: Evne til å identifisere taktikker, teknikker og prosedyrer (TTP).
 - Høy modenhet: Forståelse av strategier og attribusjon til spesifikke grupper.

Detection Maturity Leve (DML) modellen (Stillions)



APT (Advanced Persistent Threat)

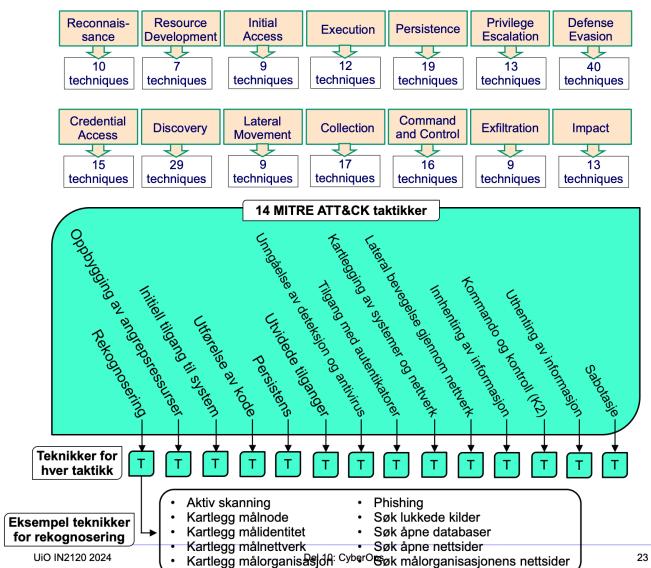
- Avansert vedvarende trussel, ofte nasjonalt støttet.
- Egenskaper
 - Avansert: Tilgang til ressurser for etterretning og utvikling av exploits.
 - Vedvarende: Langsiktige mål, utholdenhets, vanskelig å stoppe og oppdage.
 - Trussel: Har hensikt, mulighet og kapasitet til å utføre angrep.
- **Mål:** Målrettede cyberoperasjoner mot land og sektorer som forsvar, finans og helse.

MITRE ATT&CK

- En kunnskapsbase over taktikker og teknikker brukt av trusselaktører.
- Innhold:
 - Basert på observasjoner av faktiske hendelser.
 - Fokus på teknikker og taktikker, som phishing for tilgang.
 - Brukt for trusselmodellering og å forstå angrepsvektorer.

MITRE ATT&CK-matrisen

- **Struktur:** Organisert rundt teknikker (hvordan) og taktikker (hvorfor).
- Taktikk og Teknikk:
 - **Taktikk:** Formål med teknikken, f.eks. tilgang til system.
 - **Teknikk:** Metode for å oppnå taktisk mål, f.eks. phishing



CTI-kategorier (Cyber Threat Intelligence)

- **Strategisk CTI:** Beskrivelse av trusselaktører/ APT basert på aktiviteter og mål.
- **Taktisk/Operasjonell CTI:** Informasjon om verktøy og TTP-er brukt i angrep.
- **Tekniske CTI:** Indikatorer på kompromiss, som IP-adresser og domenenavn.

Kategorier av digital trusseletterretning (CTI: Cyber Threat Intelligence)

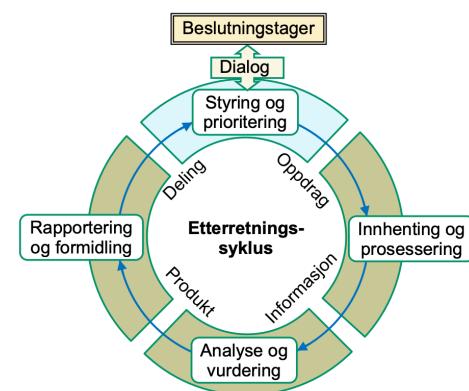


Trafikklysprotokollen (TLP) - Deling av CTI

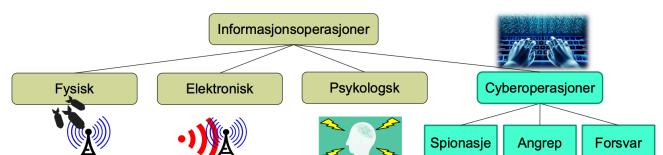
- **RØD (TLP-RED):** Personlig og begrenset til navngitte mottagere.
- **GUL (TLP-AMBER):** Begrenset deling innen organisasjon på "need-to-know"-basis.
- **GRØNN (TLP-GREEN):** Kan deles bredt innen sektoren, men ikke offentlig.
- **HVIT (TLP-WHITE):** Fri distribusjon uten begrensninger.

CTI-syklus - Prosess

- Prosess for å innhente, analysere og dele Cyber Threat Intelligence (CTI).
 - **Beslutningstager:** Initierer syklusen basert på behov. Dialog sikrer relevans.
 - **Styring og prioritering:** Bestemmer oppdrag og fordeler ressurser.
 - **Innhenting og prosessering:** Samler data fra manuelle/automatiserte, interne/eksterne kilder. Prosesserer for analyse.
 - **Analyse og vurdering:** Bruk av AI og logiske teknologier for å vurdere trusler.
 - **Rapportering og formidling:** Deler resultatet, tradisjonelt som PDF, men nye plattformer muliggjør maskinlesbar CTI.



Informasjonskrigføring



Cyberoperasjoner - aka Nettverksoperasjoner

- Nettverksoperasjoner (CNE, CNA, CND):
 - Spionasje, angrep og forsvar av nettverk.
- Cyberoperasjoner (US Cyber Operations Policy):
 - **Cyber Collection:** Innsamling av data.
 - Offensive Cyber Effects Operations (OCEO): Angrep.
 - Defensive Cyber Effects Operations (DCEO): Forsvar.

Attribusjon av Cyberoperasjoner

- Vanskeligheter med Attribusjon:
 - Ugjennomsiktighet i cyberkrigføring gjør det utfordrende å attribuere angrep.
 - Feil attribusjon kan føre til utilsiktet skade.
- Reversing av Angrep:
 - Analyse av indikatorer og CTI for attribusjon og forståelse av hensikt.
 - Utfordrende grunnet kanaliserte angrep og feilrepresentasjon.

Strategi for Cyberoperasjoner

- Offisiell Strategi:
 - Flere land har utviklet forsvarsstrategier som inkluderer cyberoperasjoner.
 - USA har en offentlig policy, mens andre land holder strategien skjult for fordeler.

Nytten av cyberspionasje og offensive cyberoperasjoner

- **Fordeler:** Billigere og mindre risikabelt enn fysisk spionasje.

Cyberspionasje

- **Effekt:** Kan lamme systemer, spesielt kritisk infrastruktur.
- **Reduksjon av skade:** God beredskap og hendelseshåndtering kan begrense konsekvensene.
- **Ressurser:** Angripere trenger betydelige ressurser, men fysiske angrep kan ofte gi samme effekt billigere.
- **Fordel for angriper:** Vanskligere å attribuere.

Offensive cyberoperasjoner

- **Bruk:** Sett i konflikter som Ukraina, nyttig kombinert med fysiske operasjoner.
- **Effekt:** Forvirrer og forstyrrer fienden ved å svekke kommunikasjon.
- Strategier for cyberoperasjoner:
- **Nødvendig:** Land må ha cyberoperasjonsstrategier i moderne forsvar.
- **USA:** Har en tydelig strategi for cyberoperasjoner.
- **Andre land:** Kan velge å holde strategier hemmelige for å beholde fordelen av usynlighet.

Russiske og Amerikanske Cyberoperasjoner

- **Russland:** Kompromittert kraftnett i vestlige land siden 2014.
 - Sabotasje mot Ukraina i 2015.
- **USA:** Kompromittert kraftnett i Russland siden 2018.
 - Lite informasjon om hvordan dette ble oppdaget.

Cyberkaperfart

- **Historie:** Legal sjørøveri fra 1600–1850, kjent som kaperfart.

- **Russland:** Putin anser ikke russiske grupper som utfører cyberangrep som kriminelle, da de ikke bryter russisk lov.

- Disse gruppene har fått "kaperbrev" til å utføre cyberangrep.

- **Paris Call for Trust and Security in Cyberspace (2018):** Feilet grunnet stormakters ønske om å utføre cyberoperasjoner og manglende håndheving.

- **FN 2024:** Forslag om traktat mot cyberkriminalitet.

Cyberkrigføring og Big Tech

- **FoxBlade-angrepet:** 23. februar 2022 oppdaget Microsofts Threat Intelligence Center en ny "Wiper"-skadeware kalt FoxBlade, brukt mot Ukraina.
 - Skadeforen slettet data fra infiserte systemer.
 - Microsoft oppdaterte virusdeteksjonssystemer innen tre timer for å blokkere FoxBlade.

Potensielle for samarbeid med Big Tech

 	OS-tilbydere (Operativsystemer) <ul style="list-style-type: none">• Programvareoppdateringer og regelmessig patching• Potensiell total kontroll over alle systemer som er online
  	CPU- og microchip-produsenter <ul style="list-style-type: none">• Spesielle triggere kan åpne bakdører• Fjernkontroll av systemplatfromer
 	Computerprodusenter <ul style="list-style-type: none">• Konfigurerer oppstart, kan bygge inn spionware under produksjon• Overvåking og styring av computerplatfromer under drift
	Skytjenester <ul style="list-style-type: none">• Passiv eller aktiv tilgang til IaaS, PaaS og SaaS• Overvåking og styring i skyen

Fremtidig Cyberkrigføring

- **Manglende regler:** Ingen internasjonale regler for cyberoperasjoner.
- **Berører alle:** Cyberkrigføring påvirker alle virksomheter.
- **Big Tech:** Viktig rolle i oppdagelse og forsvar.
- **Uforutsigbart:** Raskt endrende og vanskelig å forutsi.

Strukturer av ulike cyberorganisasjoner i verden:

