IN2120 Informasjonssikkerhet
Høst 2023

Del 10: Datanettsikkerhet og cyberoperasjoner

Gudmund Grov
Universitetet i Oslo

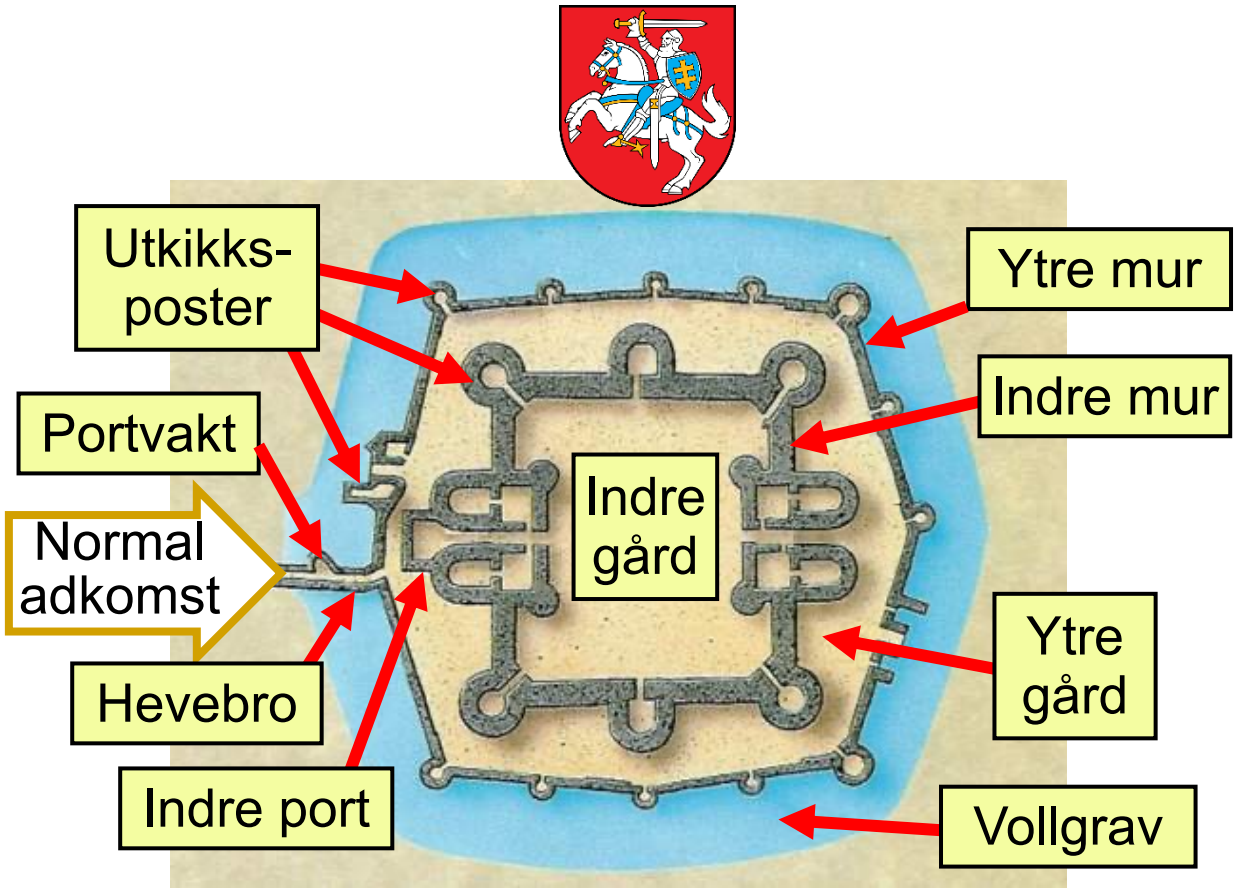
Oversikt

I denne forelesning vil du lære om

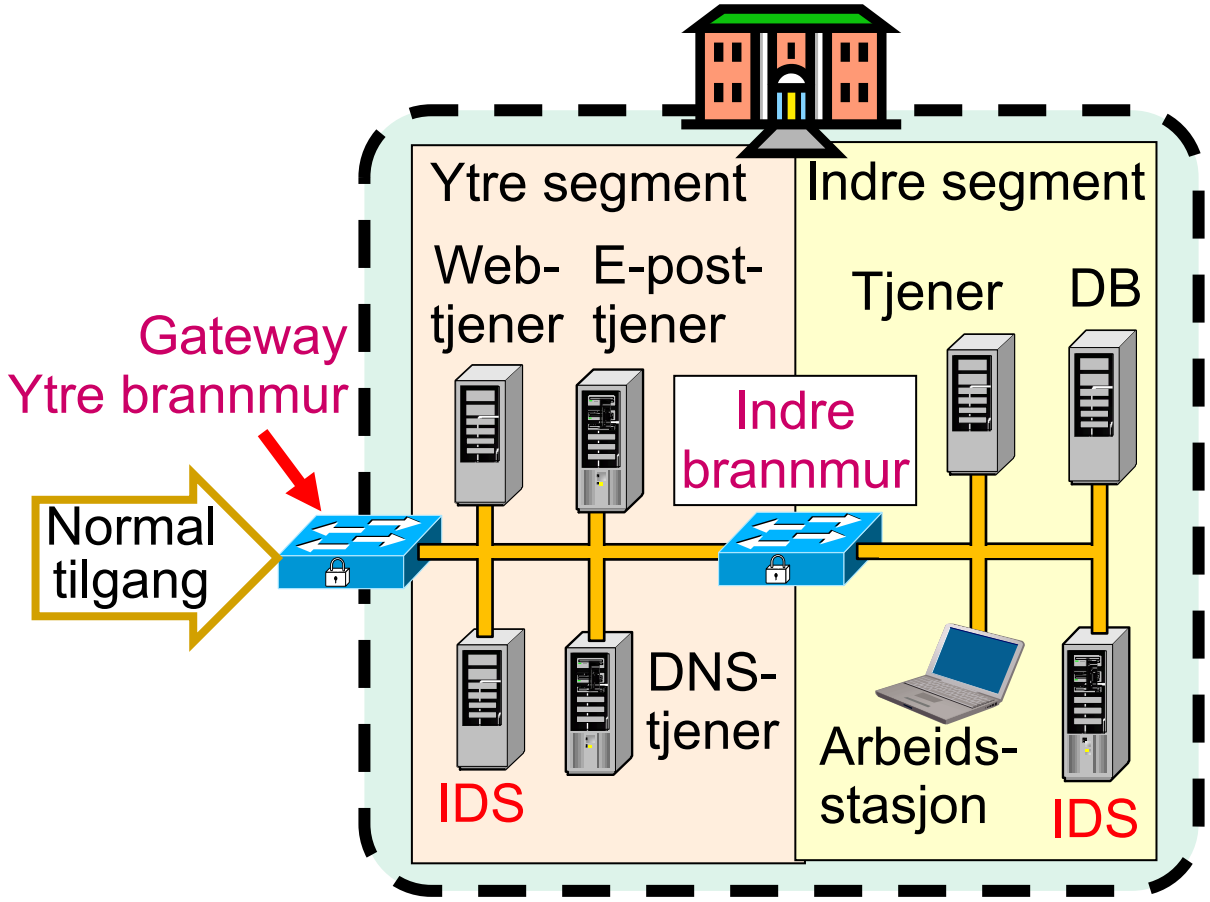
- Brannmurer
- Inntrengningsdeteksjon
- Hva et sikkerhetsoperasjonssenter (SOC) er
- TLS-inspeksjon

- Cyberoperasjoner – defensive vs. offensive
- Cyber kill chain
- Avanserte trusselaktører / Advanced Persistent Threat (APT)
- MITRE ATT&CK rammeverket

Analogi: Middelalderborg og datanett



Middelalderborg

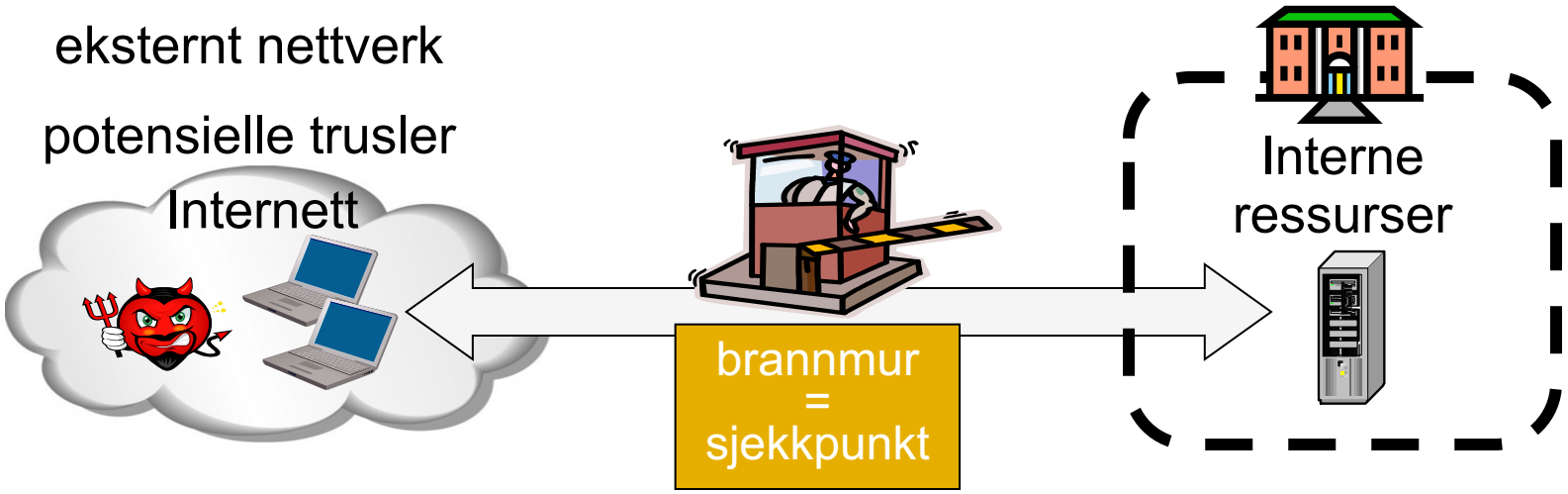


Datanett

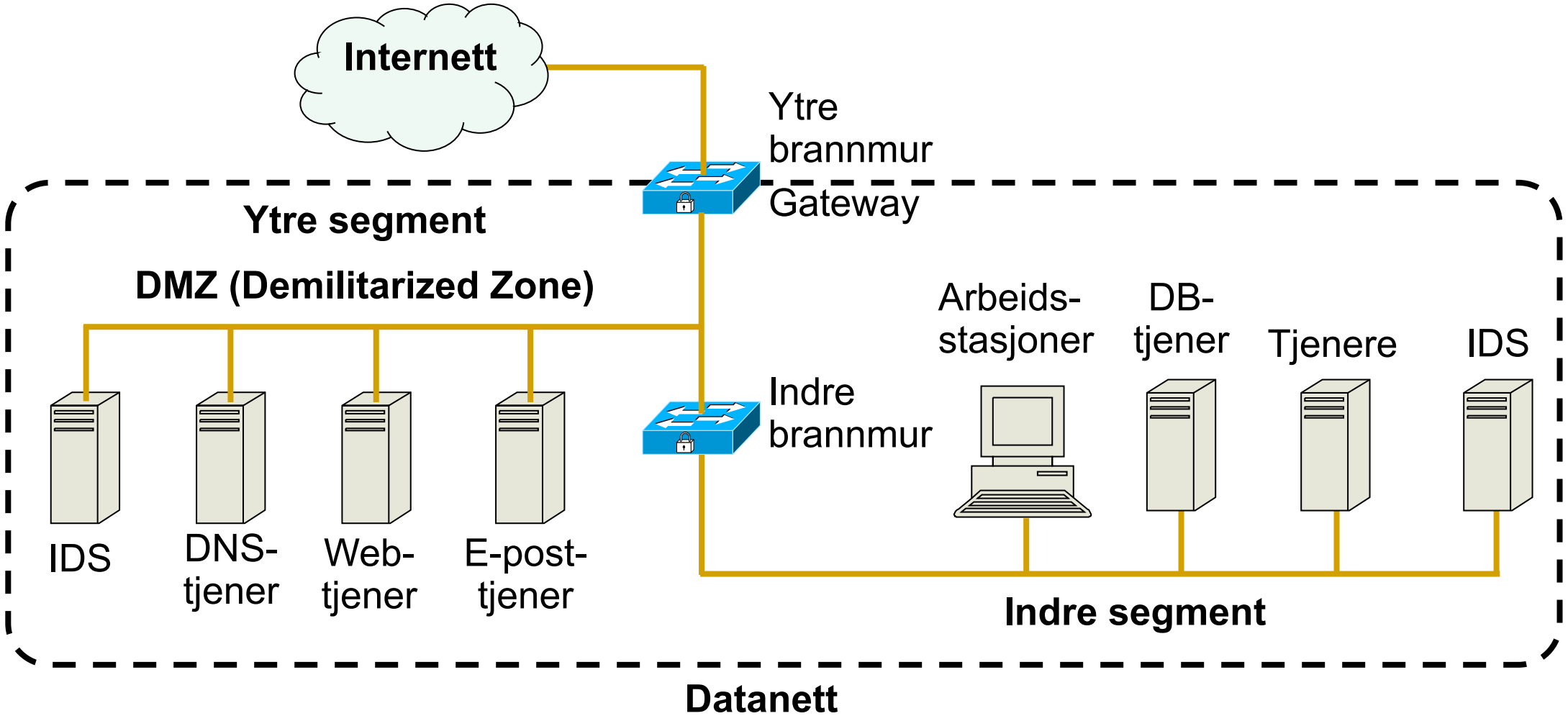
Brannmurer

Datanettsikkerhet med brannmur

- En brannmur er et sjekkpunkt som beskytter de interne nettverkene mot angrep fra eksterne nettverk (internett)
- Sjekkpunktet bestemmer hvilken trafikk som kan passere inn og ut basert på regler



Enkel datanettarkitektur med brannmurer



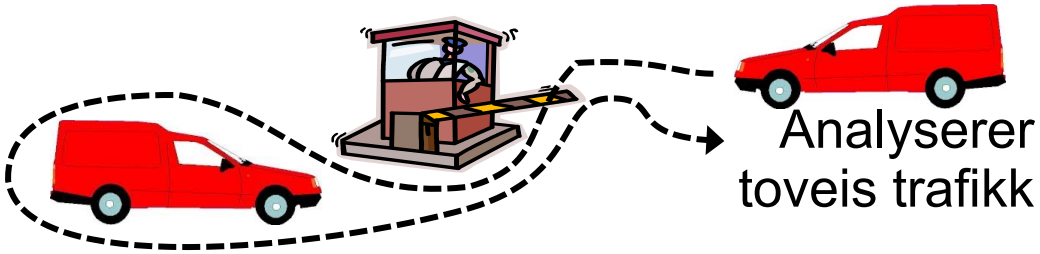
Tilstandsløse brannmurer

Inspiserer bare pakkehoder

- Enkleste type brannmur som inspiserer pakkehoder på transport- og internett-laget og basert på dette bestemmer om pakke skal godtas eller avvises
- Bruker for eksempel IP-adresse, portnummer, type transportprotokoll
- Kalles ofte for pakkefilter

- `iptables` er et mye brukt pakkefilter for Linux
  - `iptables -A FORWARD -s 131.234.142.33 -j ACCEPT`
    - Alle pakker fra (kilde) IP-adresse 131.234.142.33 aksepteres
  - `iptables -A FORWARD -p tcp -d 10.0.0.56 --dport 22 -j ACCEPT`
    - Alle TCP-pakker til (destinasjon) IP-adresse 10.0.0.56 og port 22 aksepteres

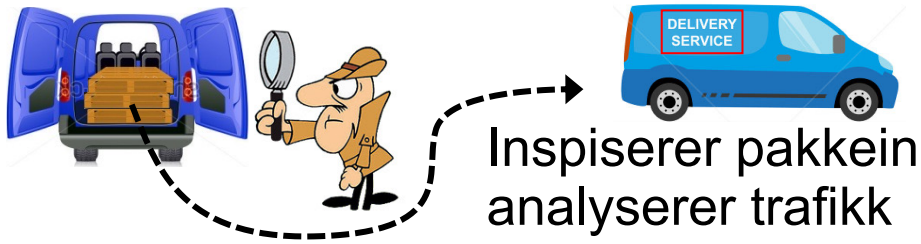
Tilstandsbaserte brannmurer



- Har oversikt over tilstanden i hver forbindelse/økt mellom klient og tjener
- Kan opprette midlertidige regler for spesifikt økt
- Mer fleksibilitet og høy ytelse men krever minne for å huske tilstand

- Eksempel: `iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT`
  - Aksepterer alle pakker som tilhørerer en etablert TCP-forbindelse eller er relatert til eksisterende UDP-kommunikasjon

Applikasjonsbrannmur



Inspiserer pakkeinnhold og analyserer trafikk

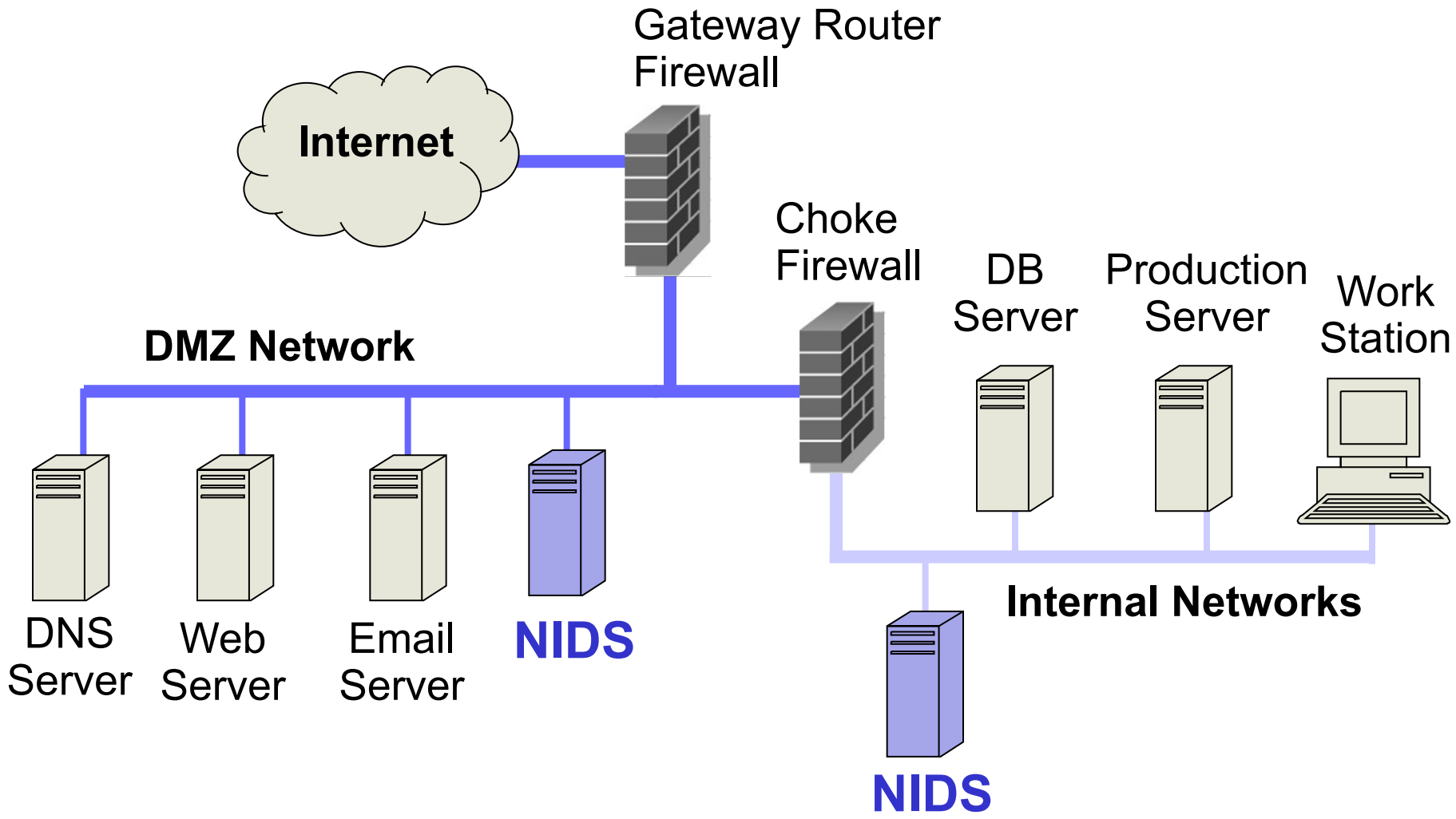
- En applikasjonsbrannmur kan inspisere brukerdata i tillegg til pakkehoder
- Støtter spesifikke applikasjonsprotokoller (HTTP,FTP,…)
- Kan konfigureres for filtrering av spesifikke brukerapplikasjoner (Youtube, Facebook,…)
- Kan filtrere ende-til-ende-forbindelse mellom klient og tjener
  - … eller i 2 deler der brannmuren spiller rollen som proxy
    - Proxy-tjener for klienten og proxy-klient for tjeneren
  - En proxy brannmur kalles ofte en gateway og brukes i VPN som vi har sett
- Applikasjonsbrannmurer med høy ytelse kalles ofte neste generations brannmurer (Next Generation Firewalls)

Inntrengningsdeteksjon

Inntrengnigsdeteksjon

- Inntrengningsdeteksjonssystemer (IDS) er systemer som forsøker å detektere mistenkelige aktivitet
- HIDS (Host-based IDS) forsøker å detektere aktivitet på vert/system den er installert
  - Overvåker prosesser, filendring, …
- NIDS (Network-based IDS) forsøker å detektere aktivitet på et eller flere nettverkssegment
  - Overvåker nettverkstrafikk
- Vi fokuser på NIDS her
- To hovedkategorier: Signaturbaserte og anomalibaserte

Inntrengningsdeteksjon i nettverk



Merk: Kan også plassere NIDS på utsiden av gateway hvis man ønsker å se all trafikk mot eget nettverk

Signaturbasert inntrengnigsdeteksjon

- Signaturbasert deteksjon
  - Kjente angrepssignaturer (beskrivelse av kjente angrep)
  - Sekvenser av systemanrop, mønstre for nettverkstrafikk, etc.
  - Kan bare oppdage kjente angrep
- Snort er en mye brukt signaturbasert NIDS
  - Eksempel signatur:

```
alert tcp $HOME_NET any -> 10.0.0.56 22
      (msg "SSH til IP-adresse 10.0.0.56")
```

    - $HOME_NET er en variabel som (typisk) inneholder IP-adresser for eget nett (som skal beskyttes)
    - Gir alarm dersom det er TCP kommunikasjon fra $HOME_NET til port 22 på IP-adresse 10.0.0.56 (Port 22 er standardport for SSH)

Eksempel på sårbarhet og Snort-regel

CVE-2017-0147 Detail

Current Description

The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to obtain sensitive information from process memory via a crafted packets, aka "Windows SMB Information Disclosure Vulnerability."

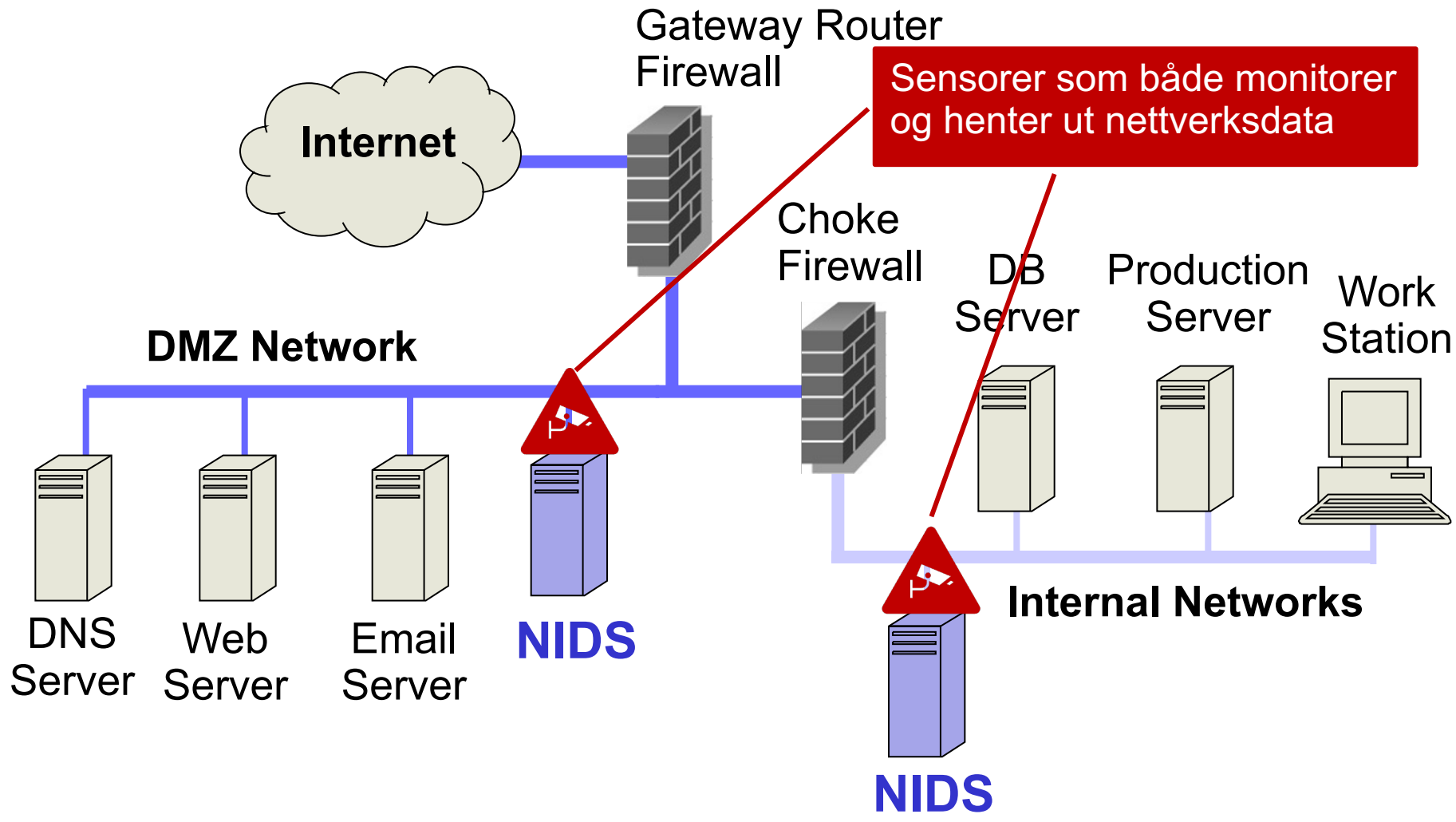
Source: MITRE
Description Last Modified: 03/16/2017
View Analysis Description


```
alert tcp $HOME_NET 445 -> any any ( msg:"OS-WINDOWS Microsoft Windows SMB possible leak of kernel
heap memory"; flow:to_client,established; content:"Frag",fast_pattern; content:"Free";
content:"|FA FF FF|"; content:"|F8 FF FF|",within 3,distance 5; content:"|F8 FF FF|",within
3,distance 5; metadata:policy balanced-ips alert,policy security-ips drop,ruleset community;
service:netbios-ssn; reference:cve,2017-0147; reference:url,technet.microsoft.com/en-
us/security/bulletin/MS17-010; classtype:attempted-recon; sid:42339; rev:2; )
```

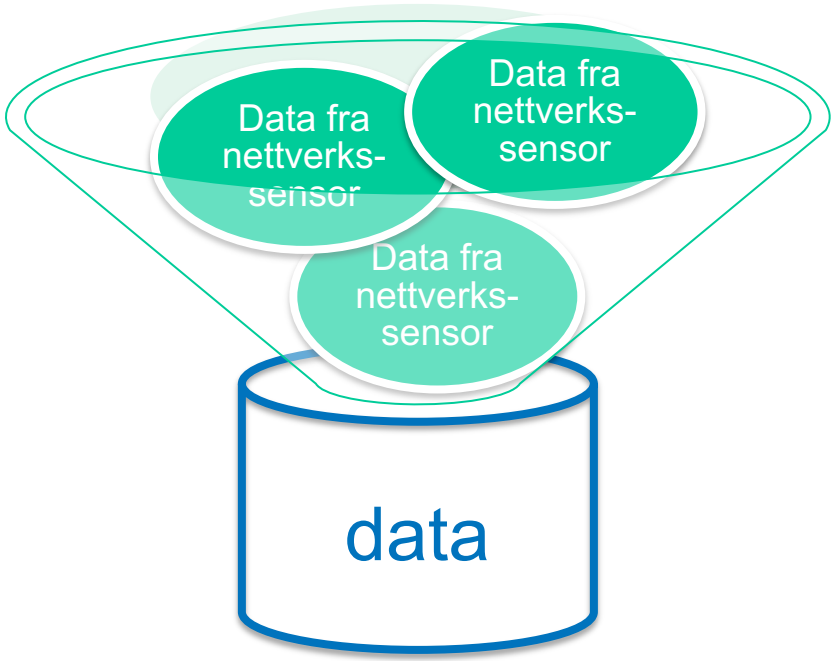
Anomalibasert inntrengnigsdeteksjon

- Signaturbasert deteksjon
  - Kan bare oppdage kjente angrep
    - (som man har signaturer for)
  - Man må (manuelt) utarbeide signaturer
  - Krever ofte at man ser innhold av nettverkspakker (deep packet inspection)
    - Kryptering (gjennom TLS) gjør dem mindre effektive
- Anomalibasert deteksjon
  - Bruker en modell for normal atferd for å oppdage avvikende atferd
  - For eksempel utløses en alarm når en statistisk sjelden hendelse oppstår
  - Ofte basert på maskinlæring
  - Kan oppdage ukjente angrep
  - ... men vil typisk gi flere falske alarmer

Anomalibasert inntrengnigsdeteksjon i nettverk

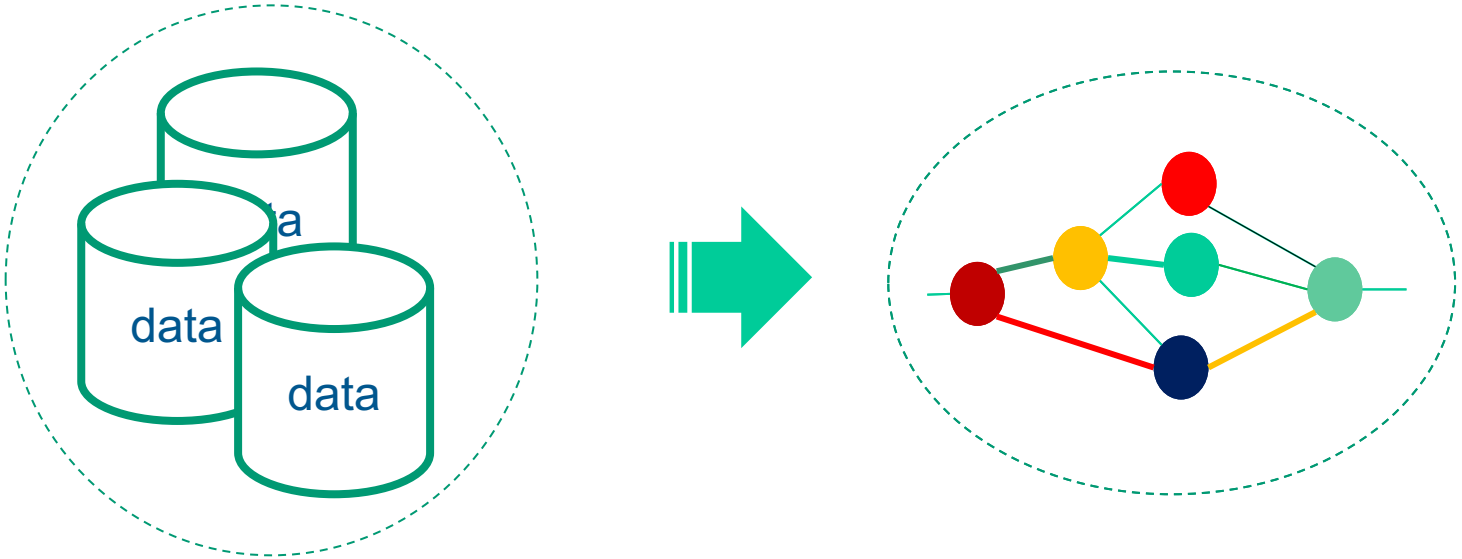


Anomalibasert inntrengningsdeteksjon: maskinlæring



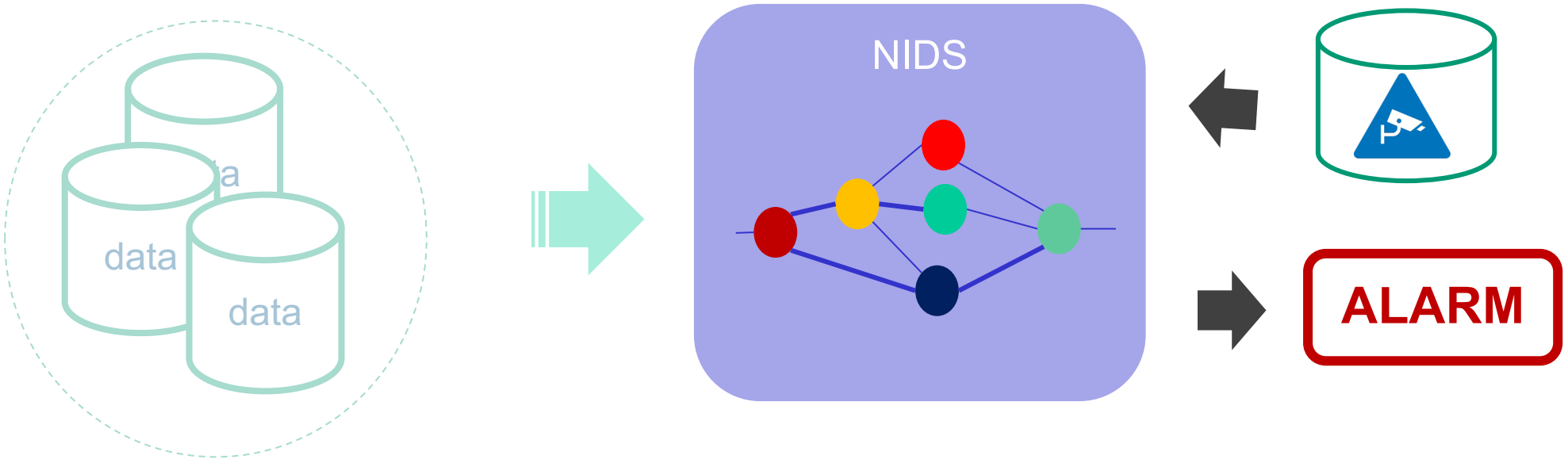
- Henter inn data fra de ulike sensorene fra ulike logger
- For større virksomheter vil det typisk gi veldig store datamengder

Anomalibasert inntrengnigsdeteksjon: maskinlæring



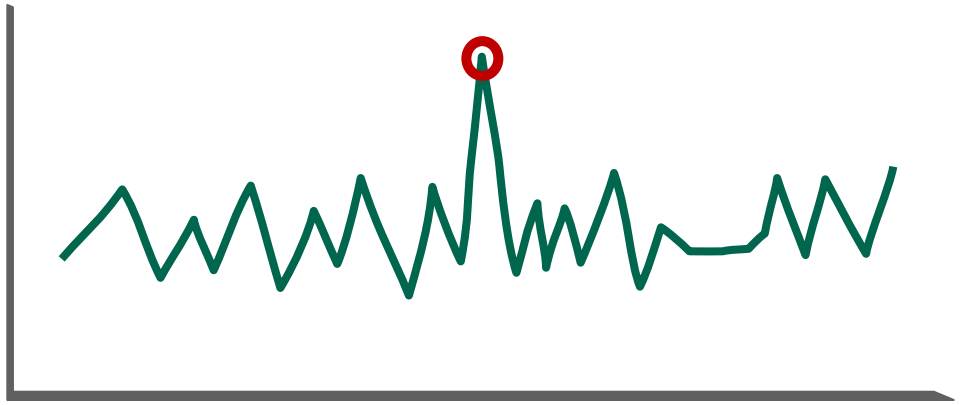
- Data brukes til å trene opp en maskinlæringsmodell
- Typisk har en slik modell mange parametere
  - Maskinlæring bruker data for å finne optimal verdi av parameterne for å kunne bruke maskinlæringsmodellen til deteksjon
  - F.eks. en modell for «normal» adferd

Anomalibasert inntrengnigsdeteksjon: maskinlæring



- NIDS bruker maskinlæringsmodellen
- Når systemet overvåker vil NIDS gi alarm basert på svar fra maskinlæringsmodellen
  - Kan for eksempel være at oppførsel observert avviker vesentlig fra normal adferd som maskinlæringsmodellen har lært.

Anomalibasert inntrengningsdeteksjon: eksempel



- Graf over kan for eksempel være nettverkstrafikk mot en tjener
- Rød sirkel indikerer et avvik (en anomali)
  - Med andre ord observeres det vesentlig mer trafikk enn normalen
- Dette kan da resultere i en alarm som må håndteres

Sikkerhetsoperasjonssenter (SOC)

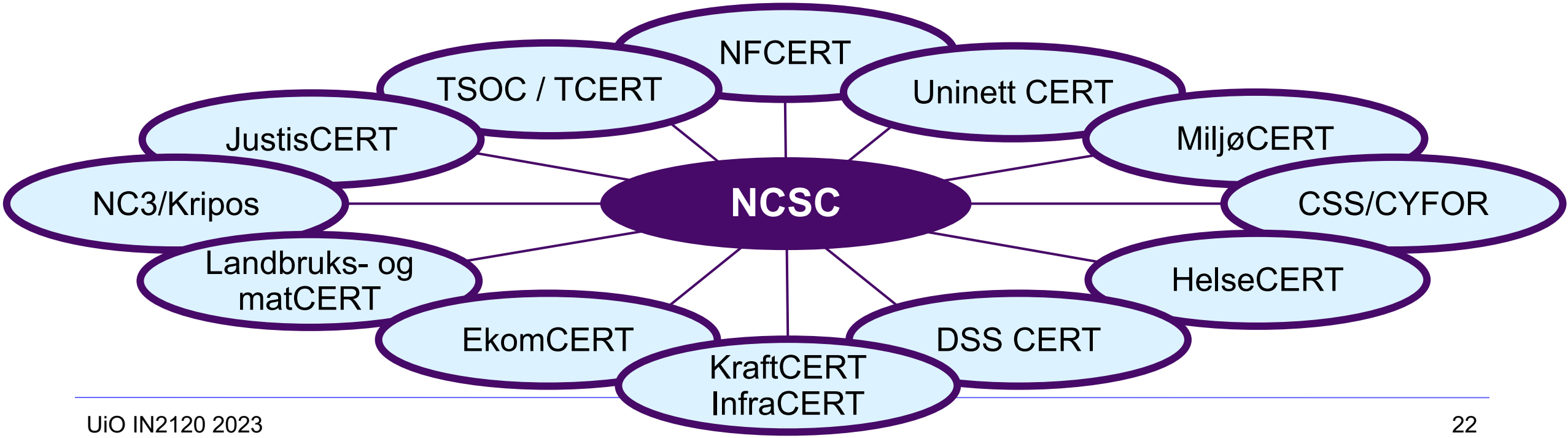
[Kilde: https://medium.com/fnplus/security-operations-center93e67268180a]

- En sentralisert funksjon eller et «team»
- Består hovedsakelig av eksperter i informasjonssikkerhet
- Organisert for å forebygge, detektere, analyse, respondere og rapportere om cybersikkerhetshendelser

- Flere lignende begreper som har lignende oppgaver/overlapp (men typisk mer fokus på respons):
  - CERT (Computer Emergency Response Team)
  - CIRT (Computer Incident Response Team)
  - CSIRT (Computer Security Incident Response Team)

NCSC og sektorvise responsmiljøer

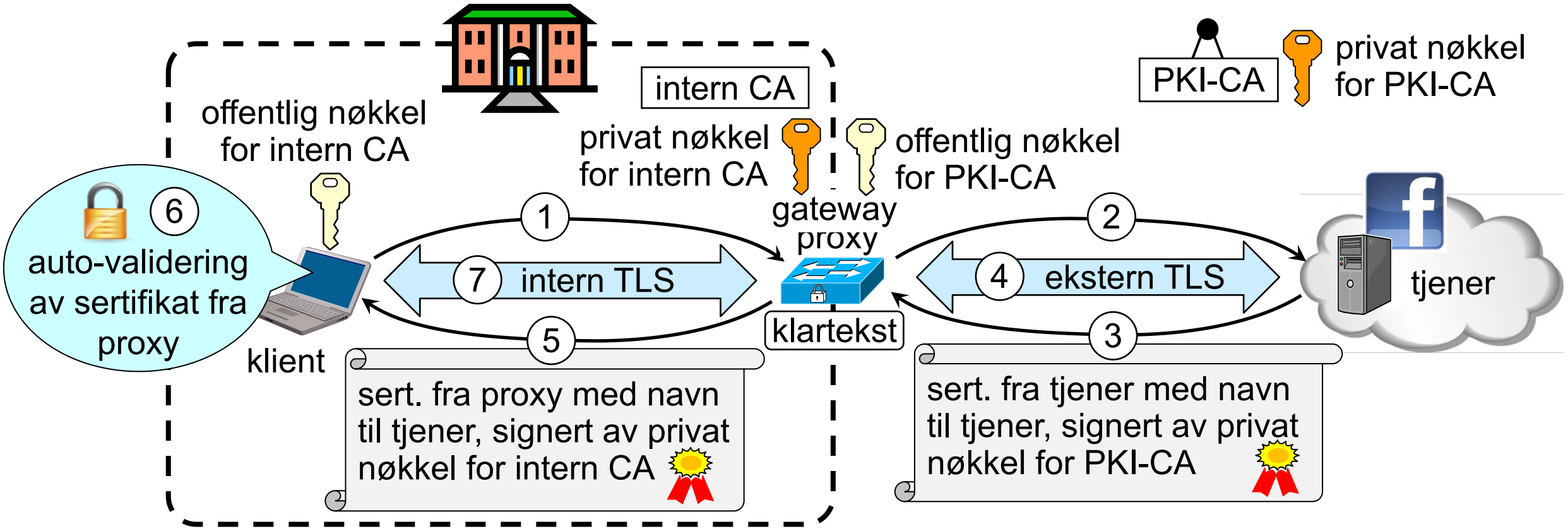
- NCSC (Nasjonalt cybersikkerhetssenter), som er en del av NSM, er nasjonal koordinerende enhet for sikkerhetshendelser med hensyn til deteksjon, hendelsesrespons og koordinering.
  - Inneholder NorCERT som er den nasjonale CERT
- I tillegg til NCSC er det opprettet en rekke sektorvise responsmiljøer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



TLS-inspeksjon

TLS-inspeksjon

- Noen organisasjoner ønsker å kunne lese kryptert HTTPS-trafikk fra ansatte
- For å bryte TLS-kryptering må gateway brannmur (proxy) utgi seg for å være ekstern tjener
- Proxy-serversertifikatet valideres automatisk av den lokale klienten, så brukeren kan tro at han/hun har TLS -tilkobling til den eksterne serveren



Cyberoperasjoner

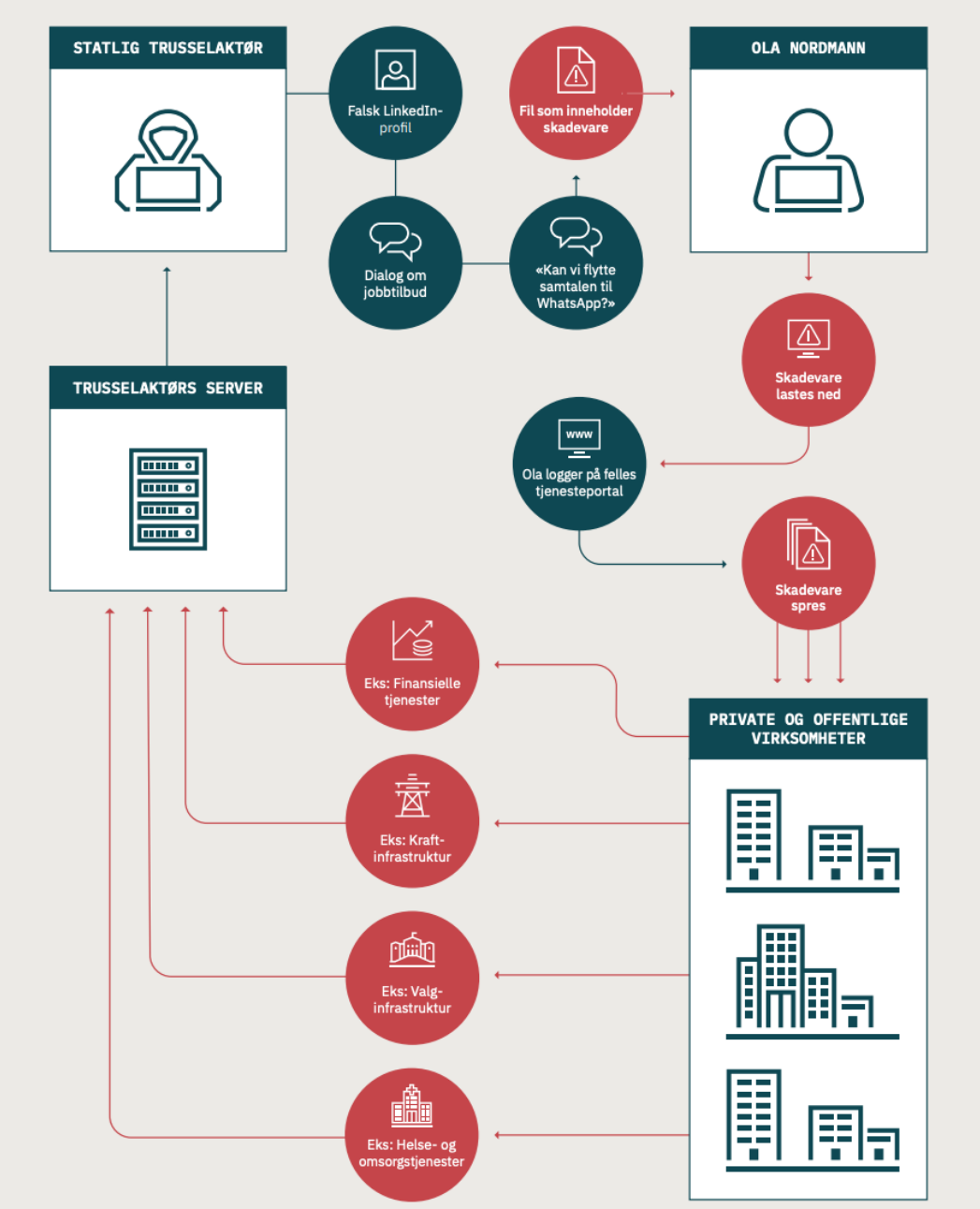
Hva er en cyberoperasjon?

- «Cyberoperasjoner» er et ganske vagt begrep som ofte brukes om forsvar og angrep av digitale infrastrukturer
- I en militær setting snakker man ofte om *offensive* og *defensive* cyberoperasjoner
- *Offensive cyberoperasjoner* brukes om uautorisert tilgang til informasjon og data i IKT-systemer (datainnbrudd). For eksempel statlige aktører eller kriminelle som bryter seg inn i systemer for vinningskriminalitet eller sabotasje.
- *Defensive cyberoperasjoner* brukes om hvordan en cyberoperasjon brukes til å håndtere disse datainnbruddene, enten noen er rammet av dem eller de har mistanke om at målrettede datainnbrudd vil skje.

Avanserte angrep/cyberoperasjoner

- Cyberoperasjoner brukes ofte om aktiviteter i digitale infrastrukturer utført av statlige aktører.
- Vi har sett flere tilfeller av disse mot norske mål, f.eks.
  - Angrep mot Stortinget (2020,2021)
  - Angrep mot Østre Toten kommune (2021)
  - Angrep mot flere (12) departement (2023)
  - *«Håndterer nytt avansert cyberangrep mot Norge» (DN i går!)*
- I nylig utgitt rapport «Nasjonalt digitalt risikobilde 2023» av NSM observer de en stor økning av cyberangrep
- Slike angrep varer ofte over lengre tid
- … og over flere steg

[nsm.no/regelverk-og-hjelp/rapporter/nasjonalt-digitalt-risikobilde-2023]

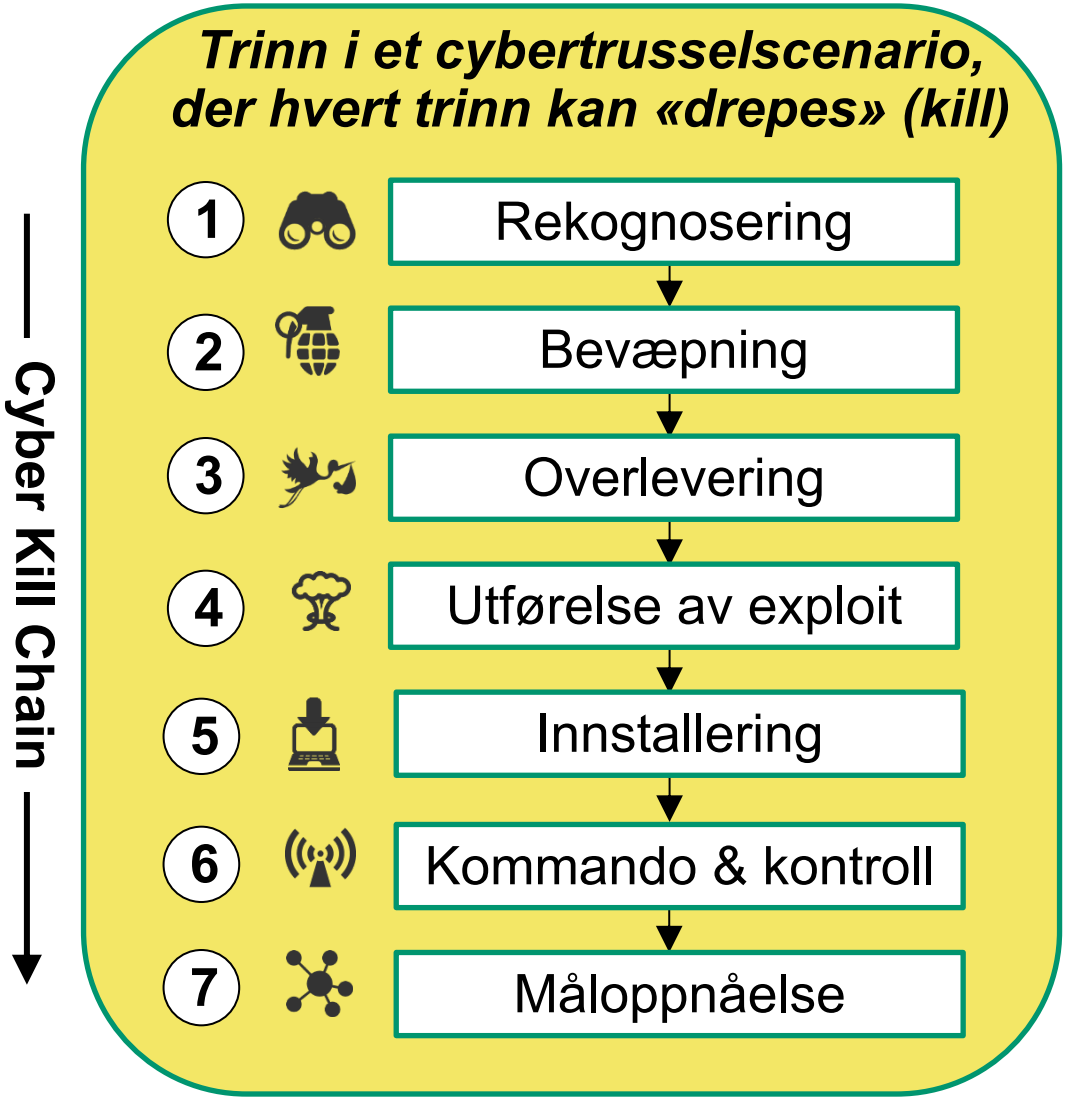


[nsm.no/regelverk-og-hjelp/rapporter/nasjonalt-digitalt-risikobilde-2023]

- Eksempel på hvordan et slikt angrep kan utføres
- Hentet fra NSMs «Nasjonalt digitalt risikobilde 2023»

Cyber Kill Chain

- Cyber Kill Chain er utviklet av Lockheed Martin.
- Den beskriver trinnene i et målrettet cyberangrep.
- Kill refererer til at angrepet kan bli stoppet/drept i hver av disse trinnene
  - Jo tidligere desto bedre



[https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html]

1. Rekognisering (cyber kill chain)

- Trusselaktøren velger ut det potensielle offeret
- Samler informasjon og «forsker» på det
- Forsøker å identifisere sårbarheter i nettverket som kan utnyttes
- Kan innebære skanning av infrastruktur, bruk av nyheter, sosiale medier, etc.

- Eksempel:
  - Et firma velges for å uthente spesifikk informasjon for bruk i vinningskriminalitet
  - Gjennom skanning av nettverket identifiser systemer som brukes og en gitt tjeneste har en kjent sårbarhet som kan utnyttes gjennom en makro i et PDF dokument
  - Gjennom annonser oppdages det at firmaet har en jobb ute på anbud
  - Gjennom LinkedIn oppdages en aktuell kontaktperson for anbudet som trolig har god systemtilgang

2. Bevæpning (cyber kill chain)

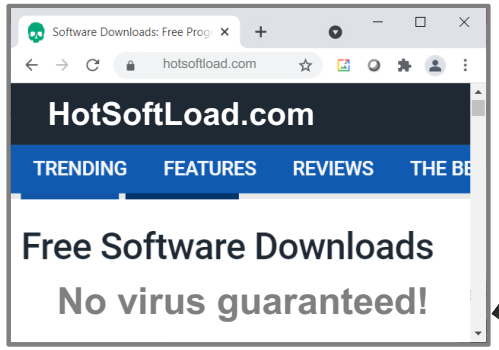
- Trusselaktøren konstruer exploit-skadevare i et egnet format som kan leveres til offeret
- Kan f.eks. utnytte en eller flere kjente sårbarheter eller nulldagssårbarheter

- Eksempel:
  - En exploit som utnytter den gitte sårbarheten lages og integreres i en PDF fil som skal imitere et reelt anbud på jobben.

3. Overlevering (cyber kill chain)

- Skadevare som ble utviklet overleveres til målet for angrepet
- Kan f.eks. være gjennom en USB, webtjener, phishing eller andre **angrepsvektorer**

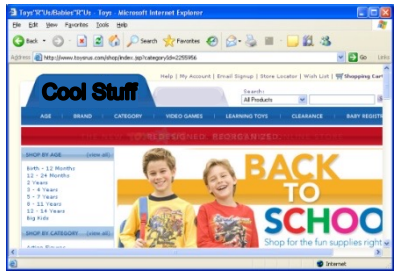
3. Overlevering: angrepsvektorer (fra tidligere)



7

Installering av skadelige programmer fra internett eller andre lagringsmedia.

Angrep

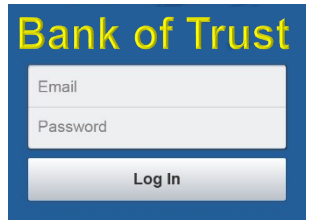


1

Drive-by-angrep fra kriminelle eller infiserte nettsider.

2

Phishing-e-post, SMS og meldinger

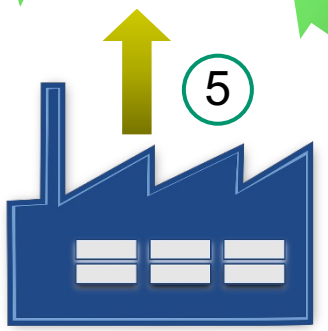


3

Falske nettsider som stjeler bruker-ID og passord.

6

Skadelige eksterne enheter.



5

Infisering og angrep gjennom leveransekjeden.

4

Direkte angrep gjennom internett.

3. Overlevering (cyber kill chain)

- Skadvare som ble utviklet overleveres til målet for angrepet
- Kan f.eks. være gjennom en USB, webtjener, phishing eller andre **angrepsvektorer**

- Eksempel:
  - En spear-phishing epost som later som å være fra en tidligere brukt leverandør opprettes
  - Sendes til identifiserte kontaktperson med PDF som vedlegg

4. Utførelse av exploit (cyber kill chain)

- Kjøring av exploit som utnytter sårbarhet i system til målet.

- Eksempel:
  - Den identifiserte kontaktpersonen ser eposten
  - Den ser reell ut så PDF åpnes for å se tilbudet
  - Dette medfører at exploit kjøres

5. Installering (cyber kill chain)

- Skadevare installeres på systemet
- En vanlig effekt av å kjøre exploit er å få åpnet en eller annen form for tilgangspunkt (f.eks. en bakdør) i form av en kommando og kontroll (K2, C2, C&C) kanal angriper kan bruke.
- Nå har angriper ekstern tilgang til det infiserte systemet.

- Eksempel:
  - Exploit kjøres og brukes til å installere seg på systemet og åpner en bakdør tilbake til angriperen
  - Angriper kan nå aksessere målets systemer gjennom K2-kanalen

6. Kommando og kontroll (cyber kill chain)

- Angriper kan utforske nettverket rundt det infiserte systemet, forplante seg videre til andre systemer (lateral movement), skjule spor og identifisere ressurser som kan stjeles/saboteres/utnyttes.
- Kommunikasjon med angriper gjennom opprettet K2-kanal

- Eksempel:
  - I dette eksempel var målet spesifikk informasjon
  - Angriper søker gjennom nettverket for å identifisere aktuell informasjon og skjuler sine spor på veien

7. Aksjon (cyber kill chain)

- Det faktiske målet med angrepet utføres
- Dette kan være uthenting av data som betyr at data samles inn, klargjøres og sendes ut av nettverket til servere som kontrolleres av angripere
- Det kan også være sabotasje, og i så fall blir ødeleggende aksjoner iverksatt.

- Eksempel
  - Angriper har nå funnet aktuelle dokumenter.
  - Det er såpass mange og de er store at disse overføres over lengre tid for å unngå at dette detekteres
  - Dette gjøres gjennom en skjult kanal mot Facebook
  - Etterpå slettes alle spor om uthentingen i systemet

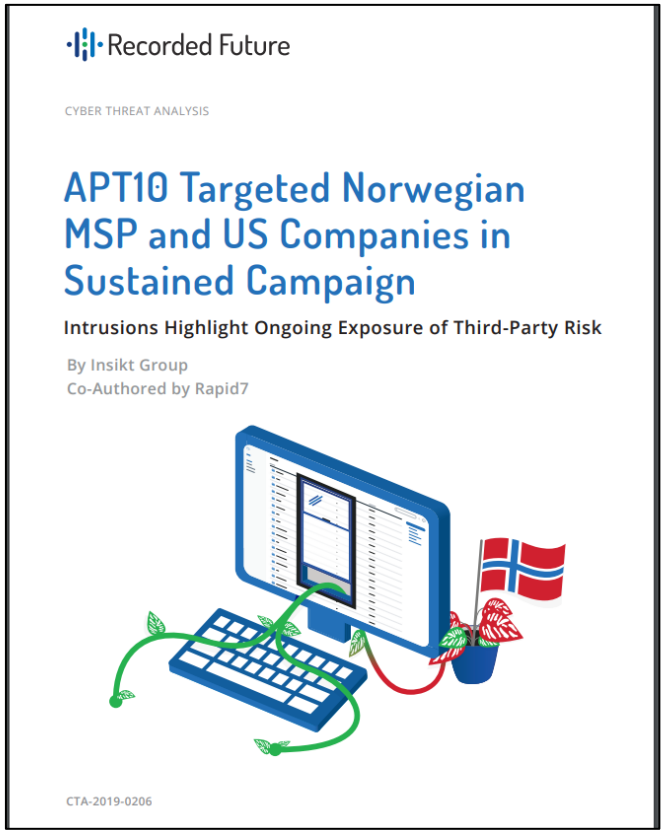
APT – Advanced Persistent Threat

- Et begrep som ofte brukes i tilknytning til det illustrerte eksempelet er APT.
- En APT (*Advanced Persistent Threat* eller *avansert vedvarende trussel*) er en trusselaktør eller gruppering.
- Tilhører ofte, eller er ofte sponset av, nasjonalstater.
- Finnes også kriminelle APT-er uten slik tilknytning til nasjonalstater.
- En APT må sees på som en gruppering med en *aktivitetsprofil.*
- Cyberoperasjoner fra APT-er er typisk målrettede mot land og sektorer (f.eks. forsvar, finans, industri, helse, energi, …).

APT – avansert og vedvarende trussel

- En APT er avansert (*Advanced*) fordi den har til rådighet rikelig med ressurser for etterretning, kompetanse og utvikling av expoits til å kontrollere infrastrukturer og utføre angrep.
- En APT er vedvarende (*Persistent*) fordi den har langsiktige målsetninger – ofte fastlagt av overordnede politiske eller strategiske enheter.
  - Betyr at den er utholdende og ikke lar seg stoppe av motstand
  - Har utholdenhet til å utføre angrep i sakte tempo
  - Går under radar og vanskeligere å oppdage
  - Cyberoperasjoner kan vare over flere år
- En APT er en trussel (*Threat*) da den har hensikt, mulighet og kapabilitet.

Beskrivelse av APTer - eksempler



- https://go.recordedfuture.com/hubfs/reports/cta-2019-0206.pdf
- https://www.mandiant.com/resources/apt1-exposing-one-of-chinas-cyber-espionage-units

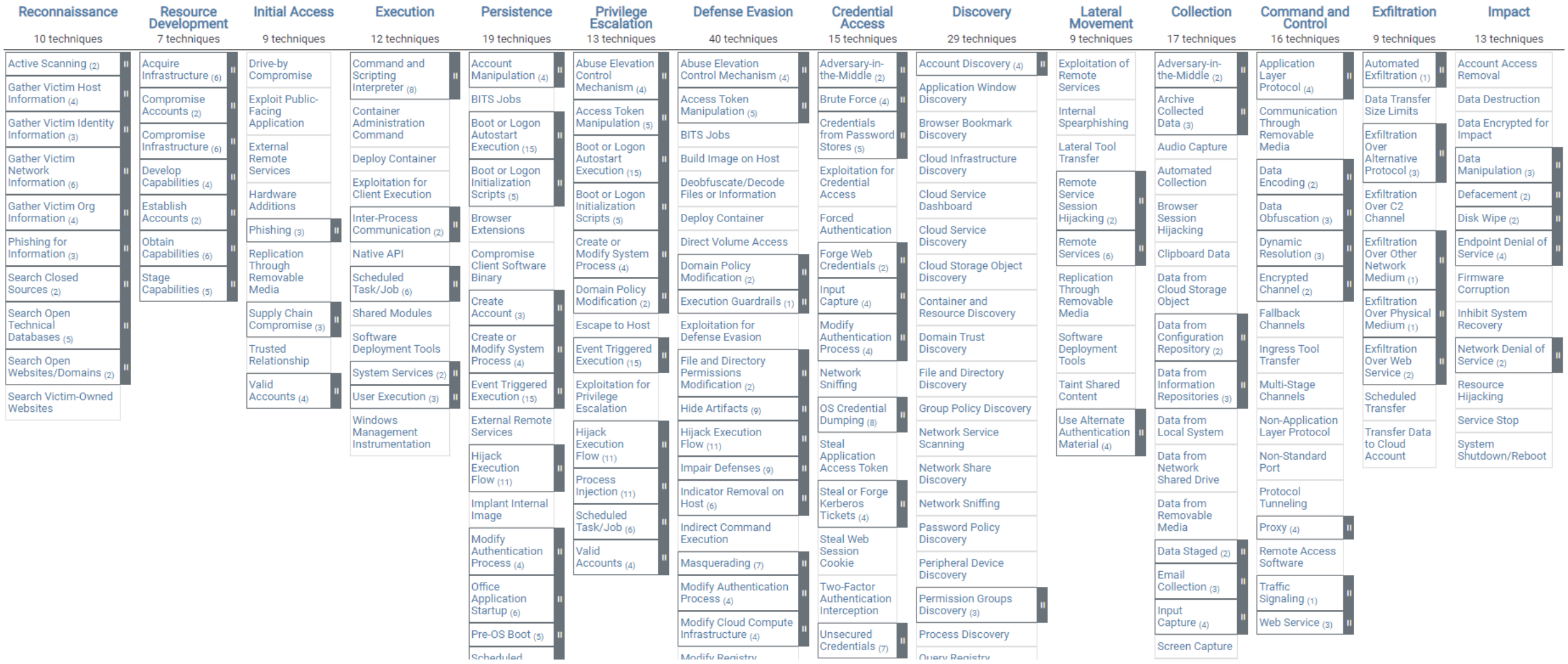
MITRE ATT&CK

- MITRE er en amerikansk (non-profit) organisasjon. Gjennom forsknings- og utviklingsaktiviteter støtter de mange amerikanske organisasjoner på ulike nivåer, i både offentlig og privat sektor, inkludert akademia.
- MITRE ATT&CK er en kunnskapsbase som strukturer taktikker og teknikker brukt av angripere og ulike APT-grupper
- Inneholder mapping av ulike APT-grupper med teknikker observert av dem
  - Basert på observasjoner av faktiske hendelser
- En viktig del av rammeverket er ATT&CK-matrisen med flere tilhørende prosjekter.
- Attack-matrisen finner dere her: https://attack.mitre.org/

MITRE ATT&CK-matrisen

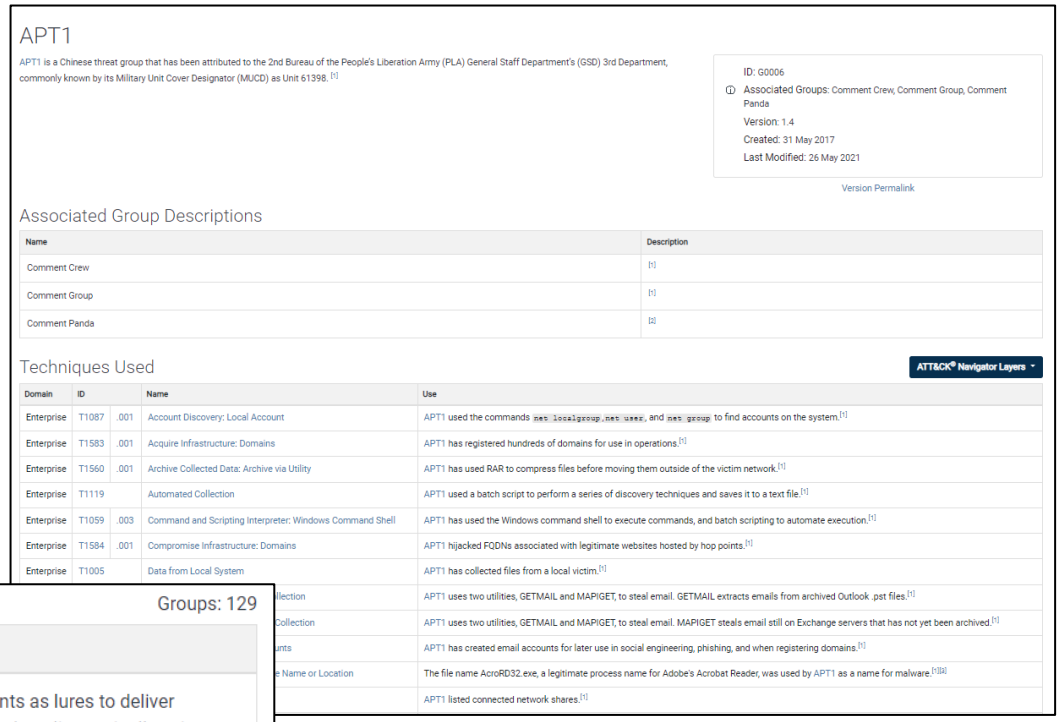
- ATT&CK matrisen er strukturert rundt teknikker og taktikker
- En *teknikk* representer her *hvordan* en angriper oppnår et taktisk mål gjennom å utføre en handling.
  - Dette kan for eksempel være phishing for å få tilgang til et system.
  - En teknikk kan være deles opp i del/under-teknikker
- En *taktikk* representerer her *hvorfor* en teknikk utføreres, med andre ord målet til angriper.
  - For eksempel er «tilgang til system» en taktikk.
- I ATT&CK-matrisen er hver kolonne en taktikk med teknikker listet under dem.

MITRE ATT&CK-matrisen



MITRE ATT&CK og APT-er

- Holder styr på ulike grupper/APT-er
  - Har per dag dato info om 129 grupper
- Mapper grupper til observerte teknikker i ATT&CK-matrisen



APT1

APT1 is a Chinese threat group that has been attributed to the 2nd Bureau of the People's Liberation Army (PLA) General Staff Department's (GSD) 3rd Department, commonly known by its Military Unit Cover Designator (MUCD) as Unit 61398. [1]

ID: G0006
Associated Groups: Comment Crew, Comment Group, Comment Panda
Version: 1.4
Created: 31 May 2017
Last Modified: 26 May 2021

Version Permalink

Associated Group Descriptions

Name	Description
Comment Crew	[1]
Comment Group	[1]
Comment Panda	[2]

Techniques Used

ATT&CK® Navigator Layers

Domain	ID		Name	Use
Enterprise	T1087	.001	Account Discovery: Local Account	APT1 used the commands `net localgroup`, `net user`, and `net group` to find accounts on the system.[1]
Enterprise	T1583	.001	Acquire Infrastructure: Domains	APT1 has registered hundreds of domains for use in operations.[1]
Enterprise	T1560	.001	Archive Collected Data: Archive via Utility	APT1 has used RAR to compress files before moving them outside of the victim network.[1]
Enterprise	T1119		Automated Collection	APT1 used a batch script to perform a series of discovery techniques and saves it to a text file.[1]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	APT1 has used the Windows command shell to execute commands, and batch scripting to automate execution.[1]
Enterprise	T1584	.001	Compromise Infrastructure: Domains	APT1 hijacked FQDNs associated with legitimate websites hosted by hop points.[1]
Enterprise	T1005		Data from Local System	APT1 has collected files from a local victim.[1]
			llection	APT1 uses two utilities, GETMAIL and MAPIGET, to steal email. GETMAIL extracts emails from archived Outlook .pst files.[1]
			Collection	APT1 uses two utilities, GETMAIL and MAPIGET, to steal email. MAPIGET steals email still on Exchange servers that has not yet been archived.[1]
			unts	APT1 has created email accounts for later use in social engineering, phishing, and when registering domains.[1]
			e Name or Location	The file name AcroRD32.exe, a legitimate process name for Adobe's Acrobat Reader, was used by APT1 as a name for malware.[1][3]
				APT1 listed connected network shares.[1]

Groups: 129

ID	Name	Associated Groups	Description
G0018	admin@338		admin@338 is a China-based cyber threat group. It has previously used newsworthy events as lures to deliver malware and has primarily targeted organizations involved in financial, economic, and trade policy, typically using publicly available RATs such as PoisonIvy, as well as some non-public backdoors.
G0130	Ajax Security Team	Operation Woolen-Goldfish, AjaxTM, Rocket Kitten, Flying Kitten, Operation Saffron Rose	Ajax Security Team is a group that has been active since at least 2010 and believed to be operating out of Iran. By 2014 Ajax Security Team transitioned from website defacement operations to malware-based cyber espionage campaigns targeting the US defense industrial base and Iranian users of anti-censorship technologies.
G0138	Andariel	Silent Chollima	Andariel is a North Korean state-sponsored threat group that has been active since at least 2009. Andariel has primarily focused its operations--which have included destructive attacks--against South Korean government agencies, military organizations, and a variety of domestic companies; they have also conducted cyber financial operations against ATMs, banks, and cryptocurrency exchanges. Andariel's notable activity includes Operation Black Mine, Operation GoldenAxe, and Campaign Rifle. Andariel is considered a sub-set of Lazarus Group, and has been attributed to North Korea's Reconnaissance General Bureau. North Korean group definitions are known to have significant overlap, and some security researchers report all North Korean state-sponsored cyber activity under the name Lazarus Group instead of tracking clusters or subgroups.

https://attack.mitre.org/groups/

Oppsummering

Du bør nå ha kjennskap til:

- Brannmurer
  - tilstandsløse, tilstandsbasert og applikasjonsbrannmur
  - `iptables`
- Inntreningsdeteksjon
  - Signaturbasert og anomalideteksjon
  - `snort`
- TLS-inspeksjon
- Sikkerhetsoperasjonssenter (SOC)
- Cyberoperasjoner
  - forskjellen mellom defensive og offensive cyberoperasjoner
- Cyber kill chain og de ulike stegene
- Mitre ATT&CK rammeverket
- Hva en APT er

Slutt på presentasjonen