Ransomware

Identify and Prevent

ran·som·ware *(de; m)*

1 kwaadaardige software die bestanden of computers vergrendelt, waarna door de verspreider losgeld wordt geëist om die vergrendeling ongedaan te maken

Agenda

- Geschiedenis van ransomware
- Bekende incidenten
- Ransomware fasen
- Ransomware voorkomen
- Ransomware detecteren

Geschiedenis van ransomware

Locker ransomware

- Geen data versleuteling
- Geen data verwijdering
- Geen data exfiltratie
- Niet gericht

Crypto ransomware v1

- Data versleuteling
- Geen data exfiltratie
- Niet gericht

Crypto ransomware v2

- Data versleuteling
- Data exfiltratie
- Gericht

Bekende incidenten | Universiteit v. Maastricht

Impact

- Ransomware uitgerold op 267 (Windows-)servers
- Onbeschikbaarheid van servers en data (24/12 – 02/01)
- Ƀ30 (€200k) aan losgeld betaald
- Lange doorlooptijd: initiële infectie op 15 okt, ransom-ware op 23 dec 2019 (69 dgn)

Aanvalsvector

- Phishing/Excel-macro
- Kwetsbaarheden

Attributie

- Clop ransomware
- TA505 (GraceRAT)

NOS Nieuws Sport Uitzendingen

NOS NIEUWS • BINNENLAND • TECH • 05-02-2020, 14:58

Hackers Universiteit Maastricht zaten maanden in netwerk; 200.000 euro betaald

Computers op de Universiteit Maastricht ANP

De hackers die de Universiteit Maastricht aanvielen, zaten ruim twee maanden in het netwerk van de universiteit. Pas daarna sloegen ze toe. Dat blijkt uit het forensisch onderzoek naar de aanval.

https://nos.nl/artikel/2321732-hackers-universiteit-maastricht-zaten-maanden-in-netwerk-200-000-euro-betaald

Bekende incidenten | Colonial Pipelines

Impact

- Pijplijn afgesloten (7 – 12 mei 2021)
- *Technische* impact blijkt uiteindelijk beperkt tot IT (geen OT impact)
- 100 GB aan data buitgemaakt
- ฿75 aan losgeld betaald, FBI weet ฿63,7 terug te halen

Aanvalsvector

- Gecompromitteerd VPN-account
- Geen MFA

Attributie

- DarkSide
- Ransomware-as-a-Service (RaaS)

Bekende incidenten | EKANS

Impact

- Data versleuteld/ mogelijk geëxfiltreerd
- Specifieke processen worden gestopt (incl. ICS):
  - GE Proficy data historian
  - GE Fanuc licensing server
  - Honeywell HMIWeb
- *Geen* capabilities om commando's te injecteren in ICS-gerelateerde processen

Aanvalsvector

- RDP
- SMBleed
- Domain policies

Targeted

- `mds.honda.com`
- `enelint.global`

Appendix A – EKANS Targeted Processes

Process	Description
bluestripecollector.exe	BlueStripe Data Collector
ccflic0.exe	Proficy Licensing
ccflic4.exe	Proficy Licensing
cdm.exe	Nimsoft Related
certificateprovider.exe	Ambiguous
client.exe	Ambiguous
client64.exe	Ambiguous
collwrap.exe	BlueStripe Data Collector
config_api_service.exe	ThingWorx Industrial Connectivity Suite, Ambiguous
dsmcsvc.exe	Tivoli Storage Manager Client
epmd.exe	RabbitMQ Server (SolarWinds)
erlsrv.exe	Erlang
fnplicensingservice.exe	FLEXNet Licensing Service
hasplmv.exe	Sentinel Hasp License Manager
hdb.exe	Honeywell HMIWeb
healthservice.exe	Microsoft SCCM
ilicensevc.exe	

https://www.dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations/

Ransomware fasen

Initiële compromittatie

Infectie via phishing, kwetsbaarheid, account take-over, …

Verkenning/laterale beweging

Herkennen slachtoffer, verkennen netwerk, compromitteren systemen

Verwijderen backups

Bestaande backups worden verwijderd (om mitigatie onmogelijk te maken)

Uitrol ransomware (op zoveel mogelijk systemen)

Malafide componenten worden “stilletjes” uitgerold binnen de infra

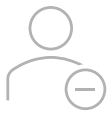
Activatie ransomware/vraag om losgeld

Organisatie krijgt plotseling te maken met uitval systemen en data

Ransomware voorkomen [1/2]

Wees voorbereid

Zorg voor draaiboeken, oefen regelmatig (bijv. table tops)



Minimaliseer het aanvalsoppervlak

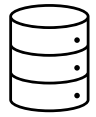
Beperk diensten, rechten, services, etc. zoveel als mogelijk

Maak gebruik van Multi Factor Authenticatie (MFA)

Zeker voor diensten die van buitenaf benaderbaar zijn

Focus op zo veilig mogelijke e-mailinfrastructuur/-gebruik

Zorg voor user awareness, e-mail filtering, content scanning, …



Zorg voor goede backups

Let op dat de backups niet bereikbaar zijn voor de ransomware!

Ransomware voorkomen [2/2]

Segmenteer het netwerk

Voorkom dat een infectie zich snel kan verspreiden

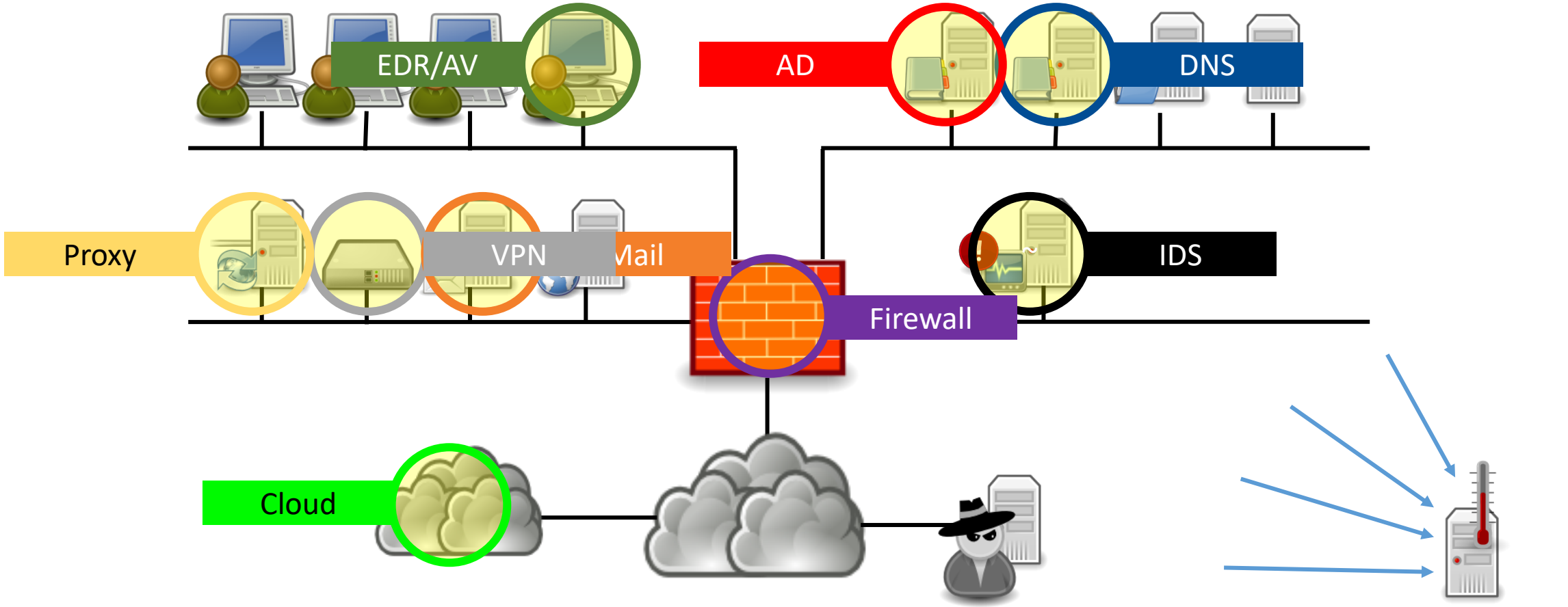
Patch (of voorkom misbruik op een andere manier)!

Zorg ervoor dat kritieke kwetsbaarheden niet misbruikt kunnen worden

Zorg voor detectie

Tijdige detectie kan de gevolgen van ransomware sterk verkleinen

Ransomware detecteren



Icons: https://www.opensecurityarchitecture.org/cms/library/icon-library

Dank voor uw aandacht!

Voor vragen kunt u terecht bij onze stand.

Sebastiaan Kors
CEO Pinewood

Niels Driesprong
Accountmanager Pinewood

Wij staan u graag te woord!

- ✔ Wees voorbereid
- ✔ Minimaliseer het aanvalsoppervlak
- ✔ Maak gebruik van MFA
- ✔ Focus op veilige e-mail
- ✔ Zorg voor goede backups
- ✔ Segmenteer het netwerk
- ✔ Patch!
- ✔ Zorg voor detectie