Ransomware attack 2019
Maastricht University (UM)

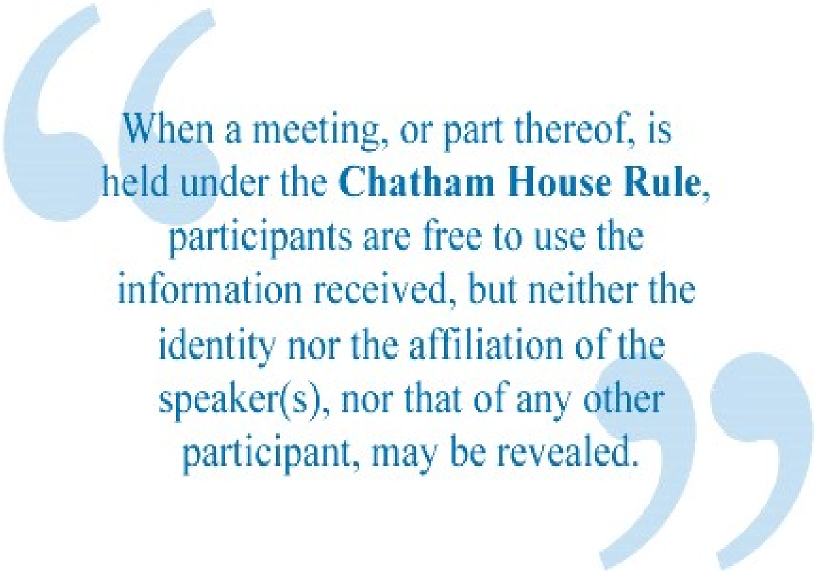
Bart van den Heuvel, CISO
bart.vandenheuvel@maastrichtuniversity.nl

Maastricht University

Interaction

Feel free to tell

Feel free to ask



When a meeting, or part thereof, is held under the **Chatham House Rule**, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.

What happened?

In short:

Maastricht University has been **Attacked**

by a

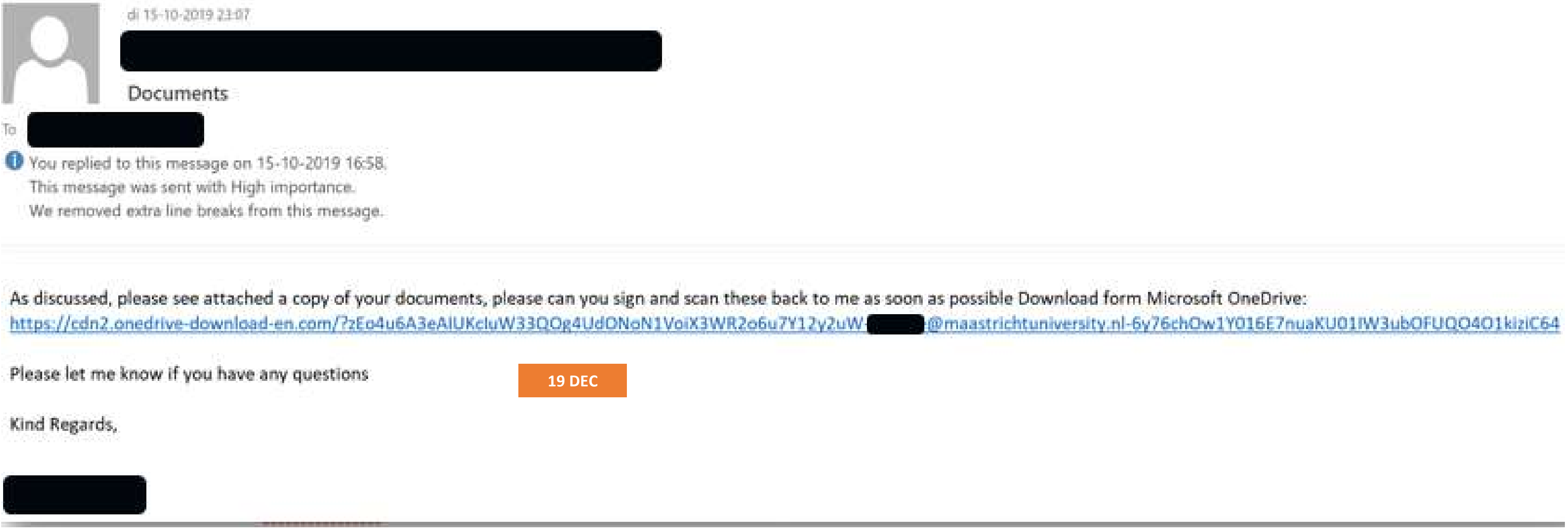
Cyber Crime Organisation !

Was UM prepared?

IS-Policy
CISO
NOZON
By-Default
IAM
Smile
Privacy-Policy
Acceptable Use Policy
By-Design
IPS
Classification
Phishing
SCIRT
DPO
Ransomware
Spam-filter
SURFaudit
OZON
McAfee
WESUS
Awareness
UM-CERT
Hora
Measures
SCIPR
SOC (io)
GDPR
Do's & Dont's
Firewall
GRC
SPLUNK

Work in Progress!

Okay, but what did really happen?



di 15-10-2019 23:07

[redacted]

Documents

To [redacted]

You replied to this message on 15-10-2019 16:58.
This message was sent with High importance.
We removed extra line breaks from this message.

As discussed, please see attached a copy of your documents, please can you sign and scan these back to me as soon as possible Download form Microsoft OneDrive:
https://cdn2.onedrive-download-en.com/?zEo4u6A3eAlUKcluW33QOg4UdONoN1VoiX3WR2o6u7Y12y2uW-[redacted]@maastrichtuniversity.nl-6y76chOw1Y016E7nuaKU01lW3ubOFUQO4O1kiziC64

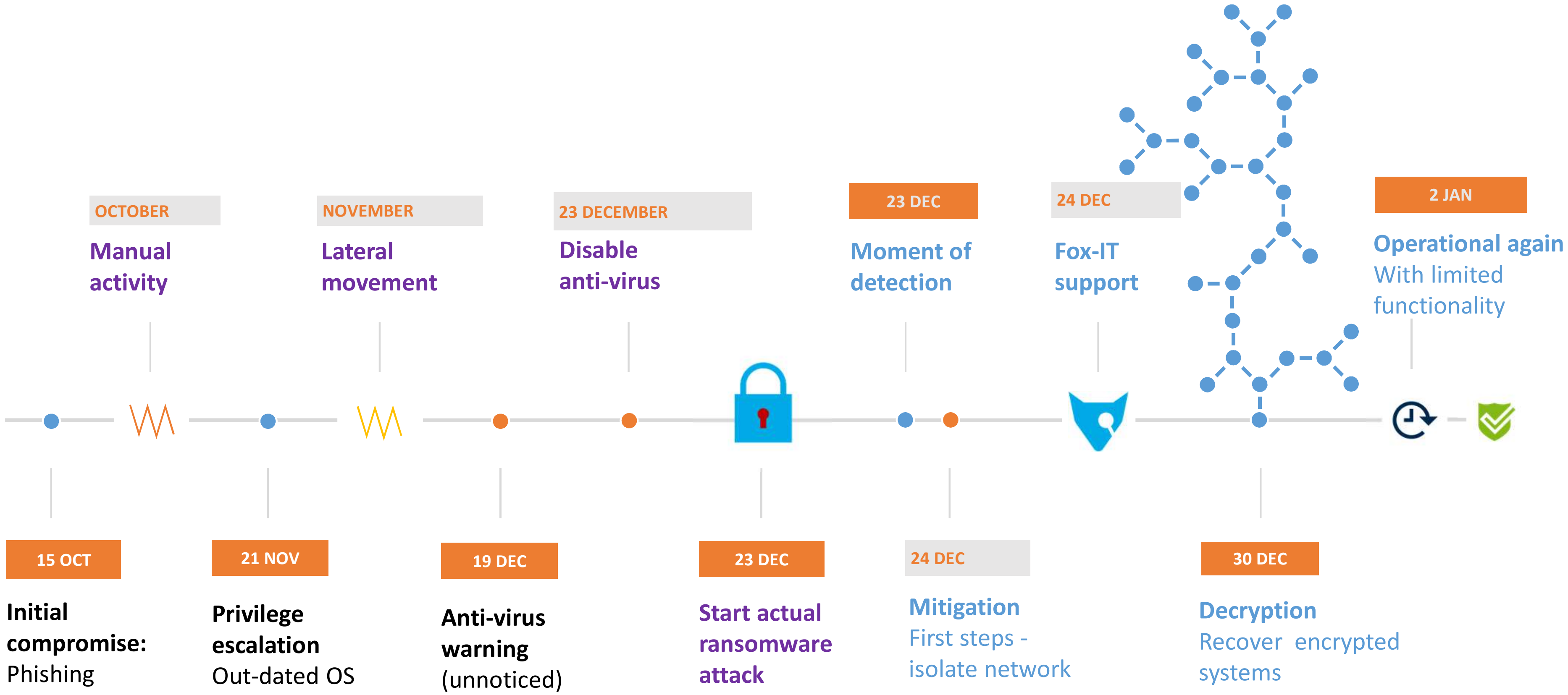
Please let me know if you have any questions

Kind Regards,

[redacted]

19 DEC

Okay, but what did really happen?



15 OCT
Initial compromise:
Phishing

OCTOBER
Manual activity

21 NOV
Privilege escalation
Out-dated OS

NOVEMBER
Lateral movement

19 DEC
Anti-virus warning
(unnoticed)

23 DECEMBER
Disable anti-virus

23 DEC
Start actual ransomware attack

23 DEC
Moment of detection

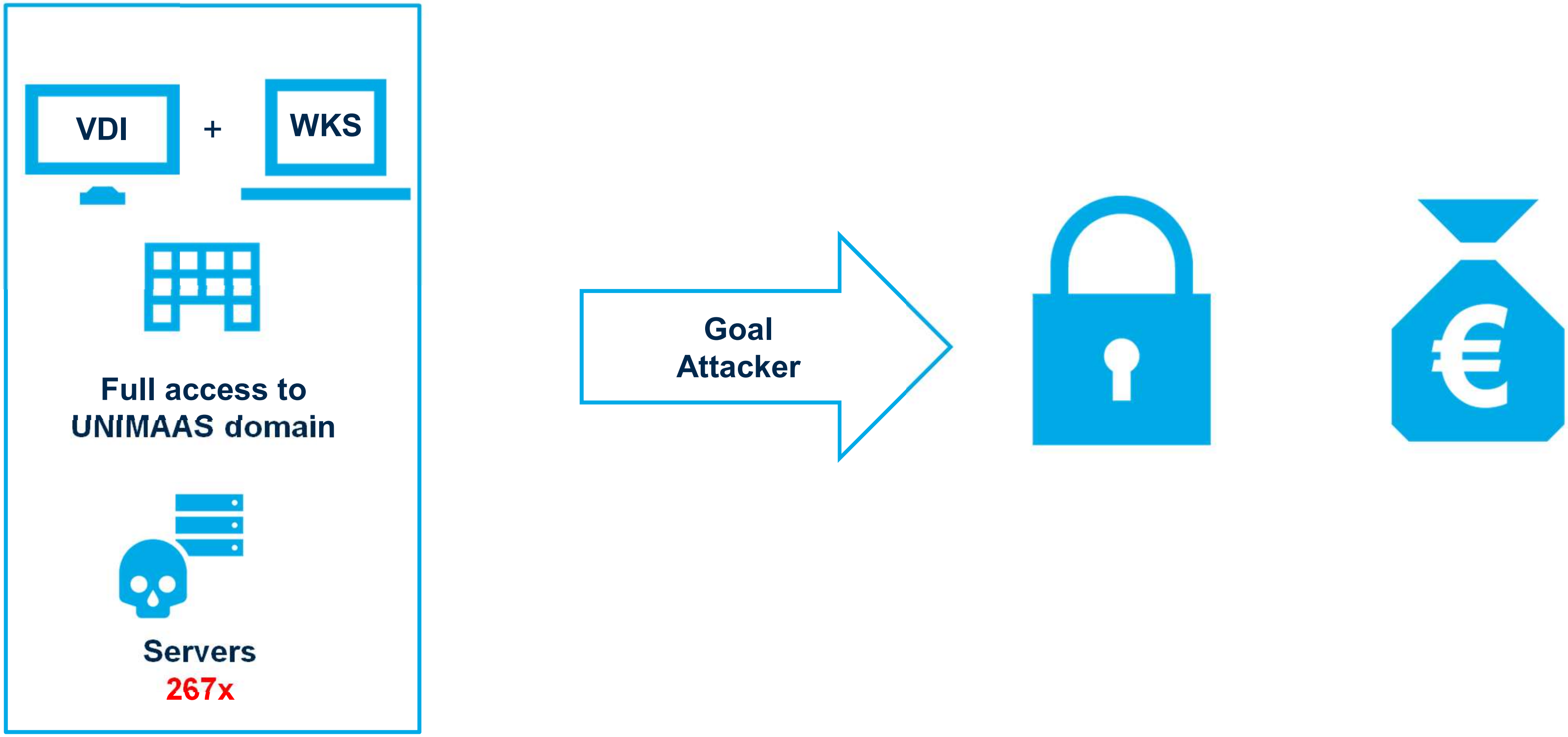
24 DEC
Mitigation
First steps - isolate network

24 DEC
Fox-IT support

30 DEC
Decryption
Recover encrypted systems

2 JAN
Operational again
With limited functionality

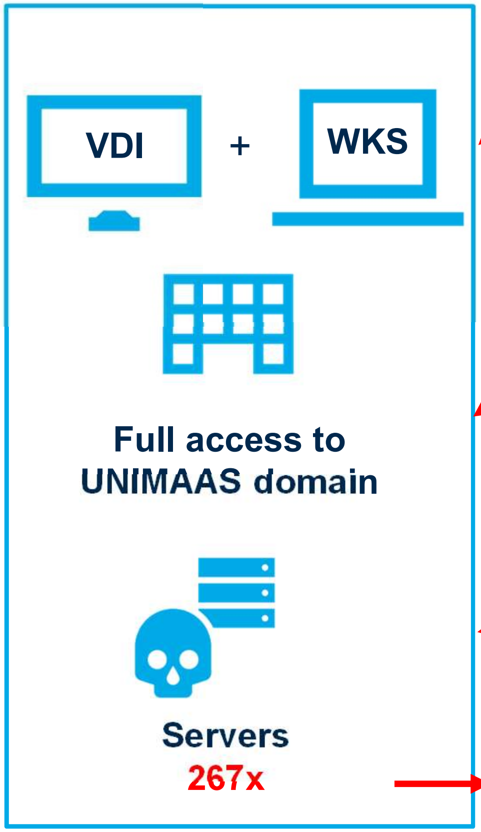
Scope vs. Goal Attacker



Modus operandi

- Grace-RAT a.k.a TA505
- Financial institutions since 2014
  - Theft of money
- Other organisations since 2017
  - Theft of money
- 150+ victims since Feb 2019
  - Clop-ransomware

Techniques



Initial attack (15 Oct)

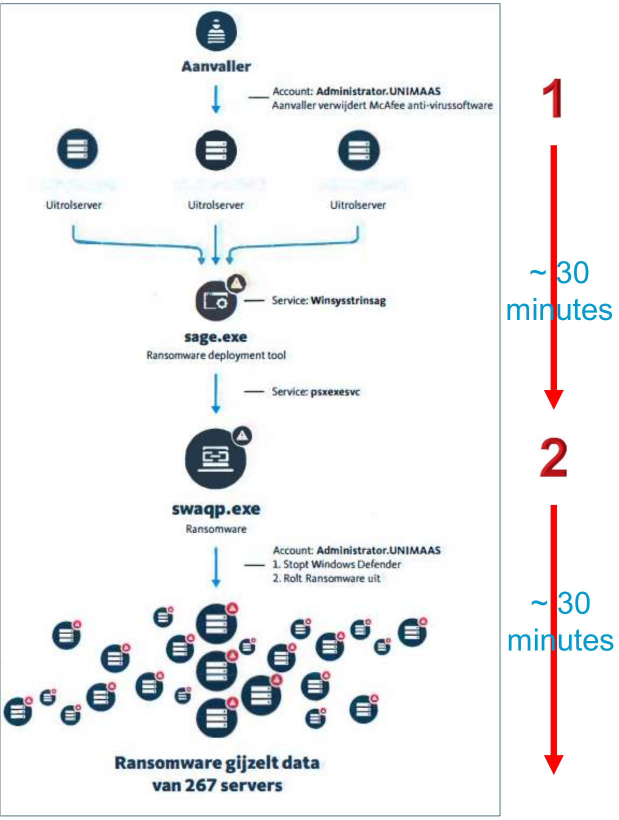
- **Phishing** (mail on Windows Clients)
- **MS-Office Macro**: **SDBBot** malware (in Reg.)
- -> contact every 15 min's (when online)

Lateral movement (Oct/Nov)

- **Meterpreter** (manual communications)
- **EternalBlue exploit** (not always confirmed)
- **PowerSploit** (PowerShell-scripts)
- **PingCastle** (-> AD structure)
- **Mimikatz** (admin access on 21 Nov)
- **Cobalt Strike**, Meterpreter & **AdFind** (on Domain Controller)

Actual ransomware attack (23 Dec)

- **sage.exe** on 3 servers (**1**: disable McAfee)
- **swaqp.exe** encrypt 267 servers (**2**: disabling Windows Defender):



Only Windows Domain-joint systems (no Unix/MacOS), including some **on-line backups**

And then: Start acting

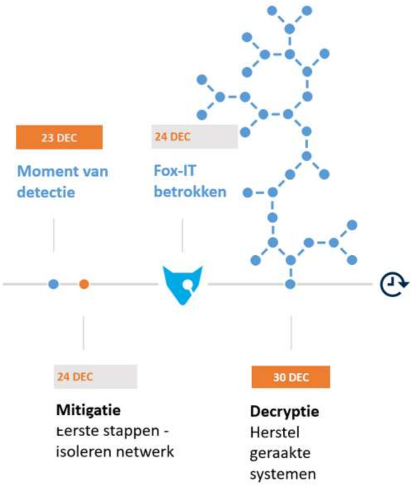
Crisis Management Team (CMT) !

FOX-IT:

- Forensics
- Monitoring: Sensors, Carbon Black, 24/7
- External Conscience (in addition to SURFcert and NCSC)

UM:

- Inventory and isolation of systems and data
- Redesign of “basic hygiene” and backup-systems
- Mitigate and rebuild
- To pay or not to pay?
- Crown jewels: Processes and data
- Official report to Police and Dutch GDPR Regulator



23 DEC
Moment van detectie

24 DEC
Fox-IT betrokken

24 DEC
Mitigatie
Eerste stappen - isoleren netwerk

30 DEC
Decryptie
Herstel geraakte systemen

How?

Communication:

- Private email, SMS, Whatsapp, Signal (without my contact list ☹)
- info@m-u.nl (thnx SURFnet !)
- Internal = External:
  - CMT, CvB, CBB, I4MU, ICTs, RvT, MT, HBO -> 150+ people involved
  - Mind you: Everything can and will become public! (Dutch law: WOB)

    → **UM chooses to be transparent and decides to go public** (as soon as possible and justified)
- Share confidential info? (UM/SURF/Uni's ->some stuff leaks to "Observant" and Tweakers)
- With the Criminals……
- Updates on UM-website (Highly appreciated)

"Mis-"communication:

- Microsoft (via HP and SURFmarket)
- SURFconext (Dutch federative infrastructure, indispensable to go live at 2 Jan)
- (Social) media: speculations, "bull-shit" (neutral to positive sentiment)

Including good stuff

- Togetherness
- Lots of treats in the coffee corner (btw coffee?)
- Lots of understanding and appreciation
- Take care of each other: mandatory day off at New years day
- Time for an occasional joke

and hassle

- Partnerlink MUMC closed immediately (understandable)
  - Temporary Security Organisation -> train new guards
  - Entrence doors in holyday configuration (create “backdoors”)
  - Coffee? No coffee: Buffer overflow in vending machines

Never waste a good Crisis

During first week

- Password reset
- Strong passwords (>15 characters) for students
- Implement planned changes (we are down anyway)
- Old tools never to be turned on again
- Close down all orphan-accounts
- Security By (re-)Design en By Default

Into the future

- Expansion of UM-SOC
- Information Security in projects
- Better tooling and procedures (including budget and personnel)
- Centralisation where feasible (policies, audit, tooling)

Lessons learned

- Awareness, awareness, awareness (management, IT-staff, users)
- Better monitoring en logging
- Incident response and Crisis management
- “Offline” backups and data recovery
- CMDB
- (micro) Segmenting our network
- Segmenting windows domain (admin structure)
- Security By Design en By Default
- Re-thinking of macro policy

Crown jewels

FOX-IT report:

- No evidence found of data exfiltration, other than network topology and credentials
- No evidence found which indicates collection of other type of data
  - Within the limited scope of the investigation
  - Given the restricted amount of available time (24 Dec. until 5 Feb.)

UM (additional investigation):

- No evidence found of data exfiltration, mutation or deletion on Student records related to financial accountability
  - Document management application (Corsa) and Fileshare with personal student files
  - Findings confirmed in external second opinion
- Work in progress:
  - Investigation of Document management Database server (Corsa)
  - Investigation of Research File share (Maastricht Study)

“Information Security and
Personal Data Protection
is no Democracy;
at best, it’s a Friendly Dictatorship”

Based on: Jaya Baloo (CISO, KPN)