Never waste a good crisis

Strategic lessons learned from the ransomware attack 2019
Maastricht University (UM)

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

Maastricht University

What happened?

In short:

Maastricht University has been **Attacked**

by a

Cyber Crime Organisation !

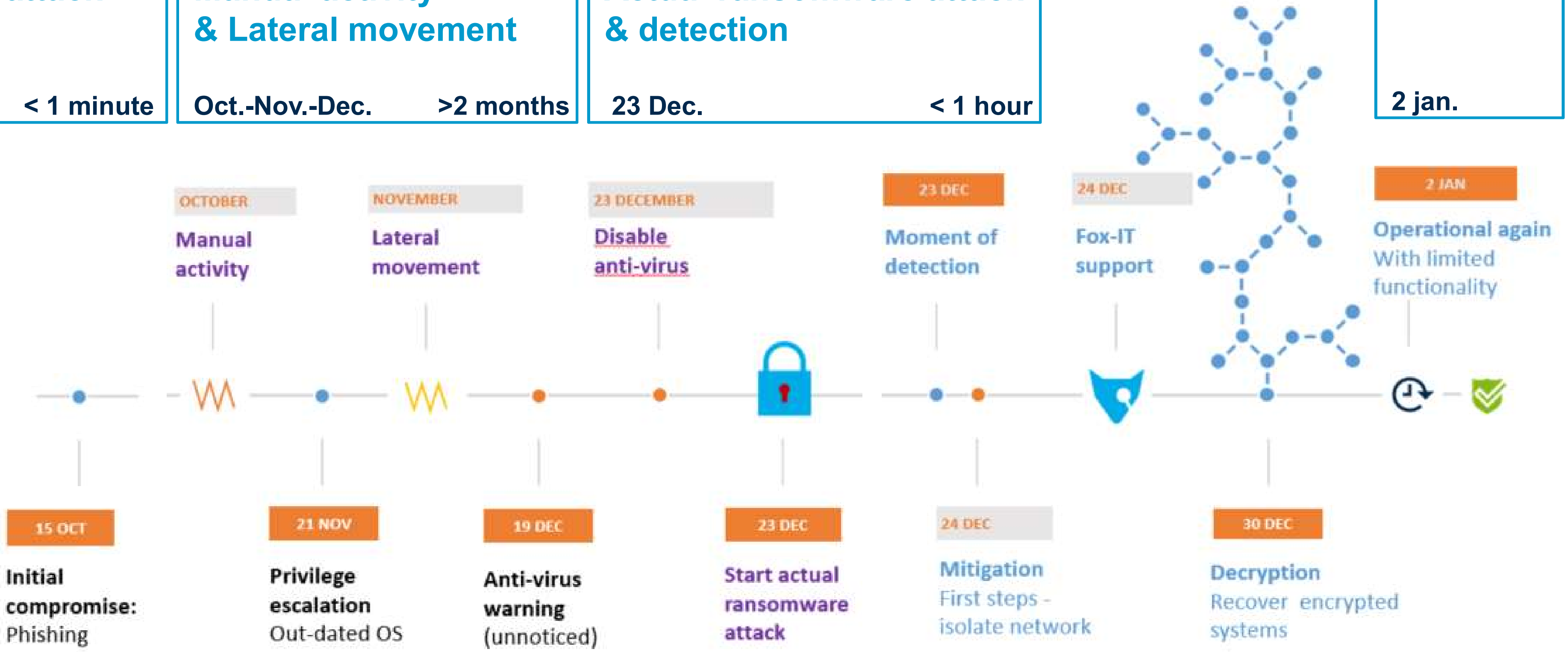
Okay, but what did really happen?

Initial attack
15 Oct. < 1 minute

Manual activity & Lateral movement
Oct.-Nov.-Dec. >2 months

Actual ransomware attack & detection
23 Dec. < 1 hour

Deadline
2 jan.



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

Crisis Management

Crisis Management Team (CMT)

FOX-IT:

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

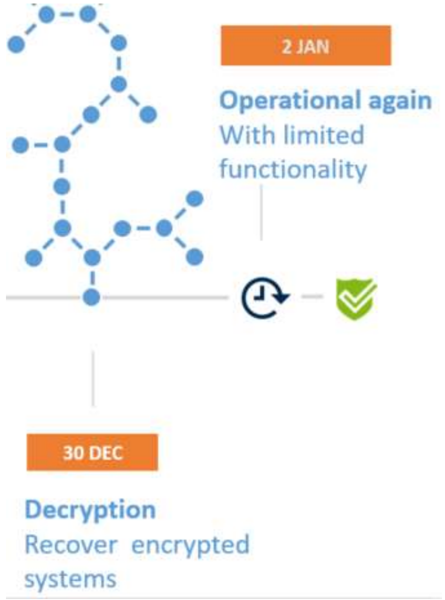
UM:

- Inventory and isolation of systems and data
- Redesign of servers and backup-systems
- Mitigate malware and rebuild systems
- Official report to Police and Dutch GDPR Regulator
- Crown jewels ? Processes and data

Deadline

Student Portals Live @ 2 Jan. 2020 (Exams @ 6 Jan. 2020)

To pay or not to pay?

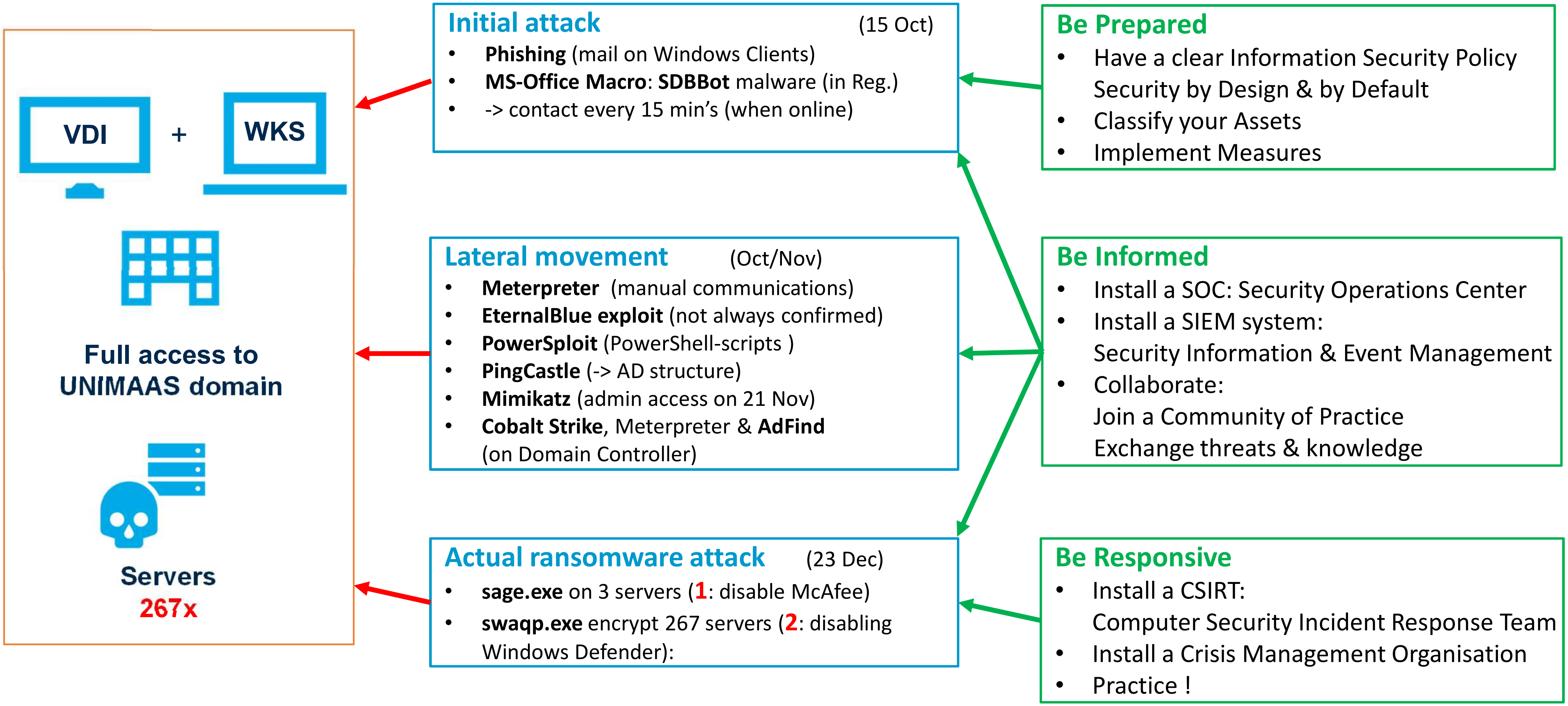


Not to pay:

Months to recover

Hugh losses

Strategic lessons



Full access to UNIMAAS domain

Servers
267x

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):

Be Prepared

- Have a clear Information Security Policy
  Security by Design & by Default
- Classify your Assets
- Implement Measures

Be Informed

- Install a SOC: Security Operations Center
- Install a SIEM system:
  Security Information & Event Management
- Collaborate:
  Join a Community of Practice
  Exchange threats & knowledge

Be Responsive

- Install a CSIRT:
  Computer Security Incident Response Team
- Install a Crisis Management Organisation
- Practice !

So, was UM prepared?

Be Prepared

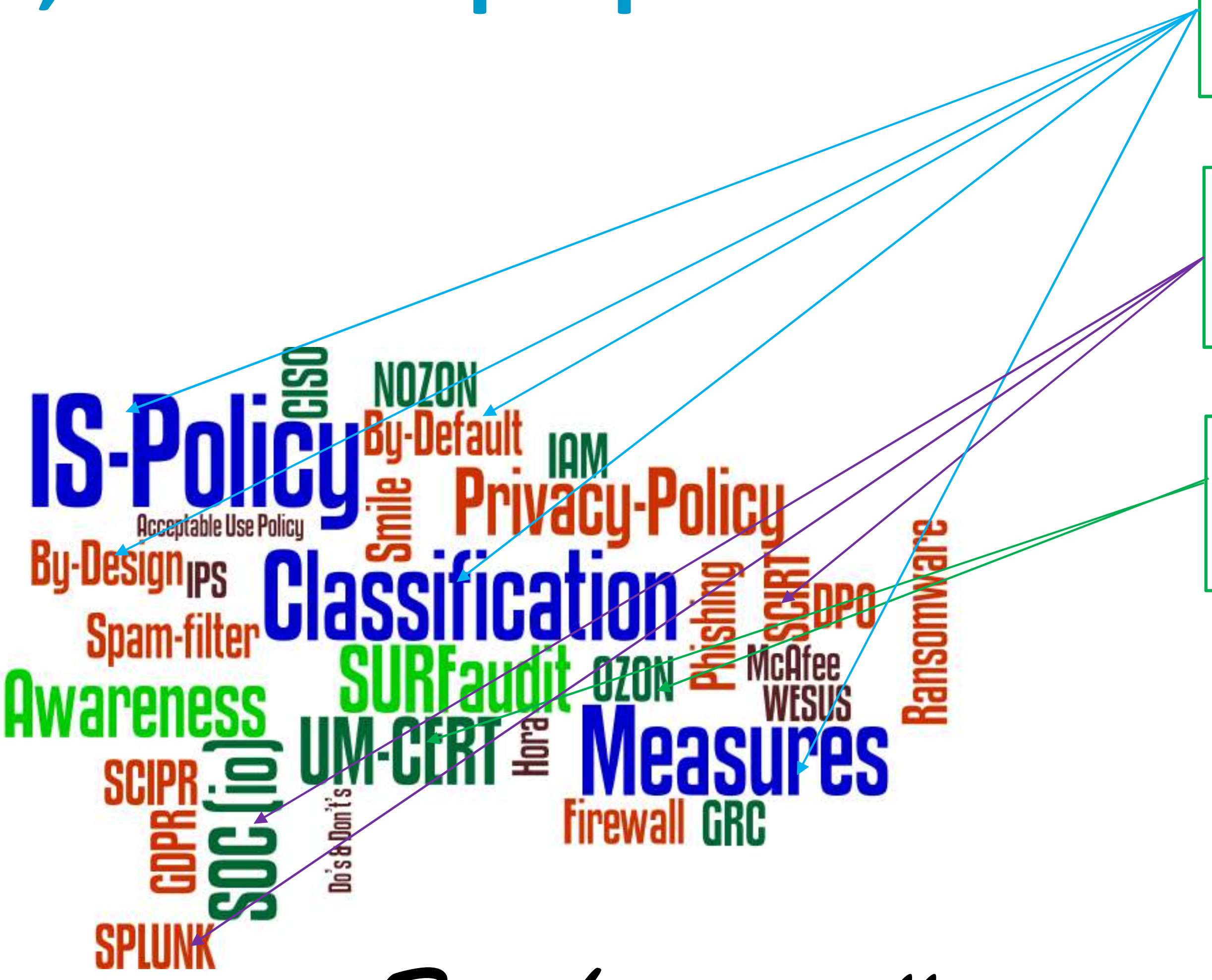
- Security Policy: by Design & by Default
- Classify your Assets
- Implement Measures

Be Informed

- SOC
- SIEM
- Community of Practice

Be Responsive

- CSIRT (or CERT)
- Crisis Management Organisation
- Practice !



But this was all.......

Work in Progress!

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

Based on: Jaya Baloo

Bonus Slides

Lessons learned

- Awareness, awareness, awareness (users, IT-staff, management)
- 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
- New macro policy

Crown jewels: Student and research data

FOX-IT report:

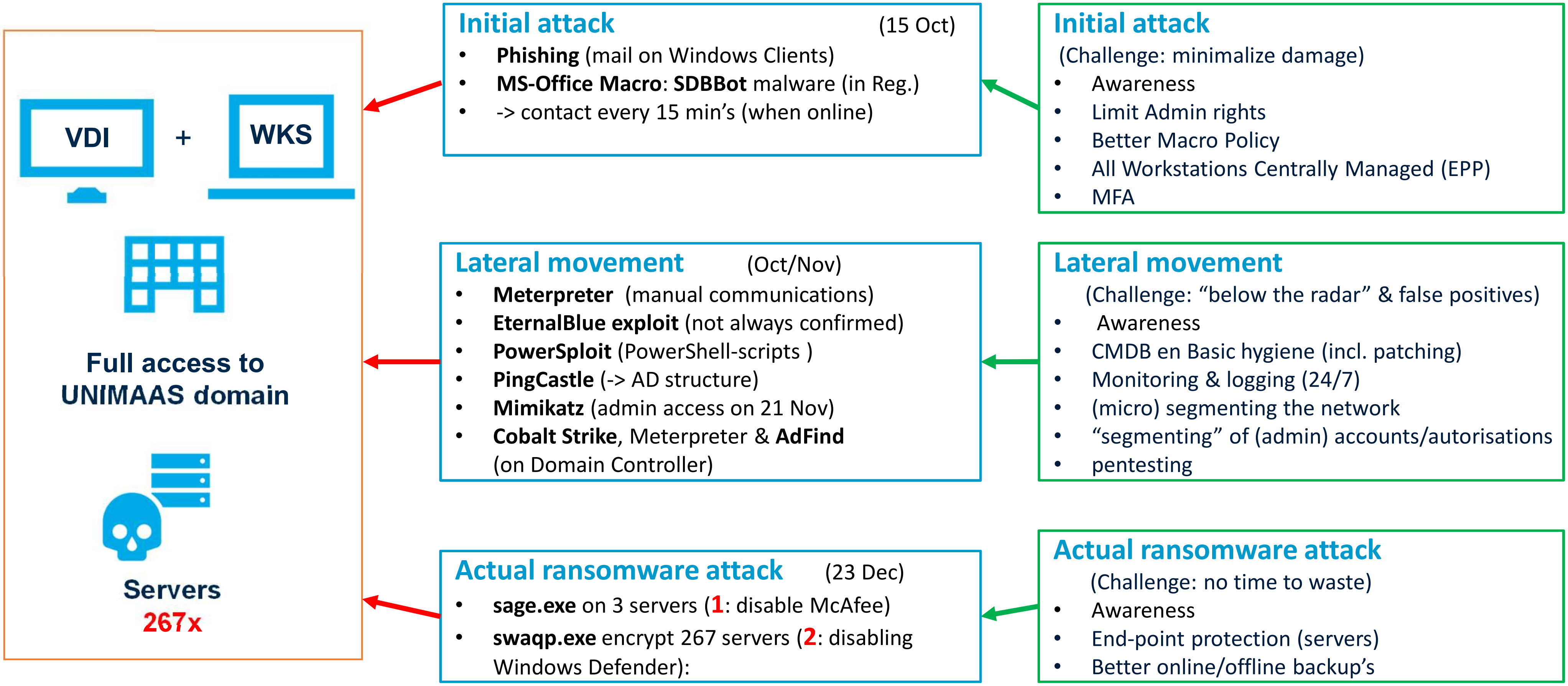
- No evidence found of data exfiltration, other than network topology and credentials
- No evidence found which indicates collection of other type of data
  - Within the limited scope of the investigation
  - Given the restricted amount of available time (24 Dec. until 5 Feb.)

UM (additional investigation):

- No evidence found of data exfiltration, mutation or deletion:

1) on Student records related to financial accountability (spring 2020, Forensics)
   - Document management application (Corsa) and Fileshare with personal student files
   - Findings confirmed in external second opinion
2) on Document management Database server (Corsa, Summer 2020, Forensics)
3) on Research File share (Maastricht Study, Summer 2020, technical risk assessment)
4) on Dark Web (Summer/Autumn 2020 , Research Project investigating 12 Marketplaces)

Improvement Plan vs. Cyber Attack



VDI + WKS

Full access to UNIMAAS domain

Servers

267x

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):

Initial attack

(Challenge: minimalize damage)

- Awareness
- Limit Admin rights
- Better Macro Policy
- All Workstations Centrally Managed (EPP)
- MFA

Lateral movement

(Challenge: "below the radar" & false positives)

- Awareness
- CMDB en Basic hygiene (incl. patching)
- Monitoring & logging (24/7)
- (micro) segmenting the network
- "segmenting" of (admin) accounts/autorisations
- pentesting

Actual ransomware attack

(Challenge: no time to waste)

- Awareness
- End-point protection (servers)
- Better online/offline backup's