Never waste a good crisis

Strategische lessen en vervolgstappen na de ransomware aanval 2019

Universiteit Maastricht (UM)

Bart van den Heuvel,
CISO UM tijdens de hack

Maastricht University

PO/VO/Speciaal Onderwijs vs. MBO/HO*

DISCLAIMER:
getallen zijn NIET getoetst, slechts als beeldvorming

Sector	Generiek	Specifiek	SAAS / Online Services	On-Premise
WO	60 %	40 %	50 % (>)	50 % (<)
HBO*	70 %	30 %	60 % (>)	40 % (<)
MBO*	80 %	20 %	80 % (>)	20 % (<)
PO/VO/SO	90 %	10 %	> 90 %	< 10 %

Verantwoordelijkheid kun je niet outsourcen !

*) een grote MBO/ROC is groter dan menig HBO en kleine HBO's zijn vergelijkbaar met MBO

Interactie

Vraag vrijuit

Wanneer een vergadering, of een deel daarvan, wordt gehouden onder de Chatham House Rule zijn de deelnemers vrij om de ontvangen informatie te gebruiken, maar noch de identiteit noch de connectie van de spreker(s), noch die van een andere deelnemer, mag worden onthuld.

https://www.chathamhouse.org/about-us/chatham-house-rule

Vertel vrijuit

[Fragment NOS journaal 27 december 2019, 20:00 uur]

Orgineel:
https://youtu.be/0XtMqT_dzfg

https://www.youtube.com/watch?v=0XtMqT_dzfg

Ingekort en met ondertiteling:
https://youtu.be/ffQfiEutIUo
https://www.youtube.com/watch?v=ffQfiEutIUo

(de MP4 versie lokaal opgeslagen is beter van kwaliteit)

Oké, maar wat gebeurde er nu echt?

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-6y76chOw1Y016E7nuaKU01IW3ubOFUQO4O1kiziC64

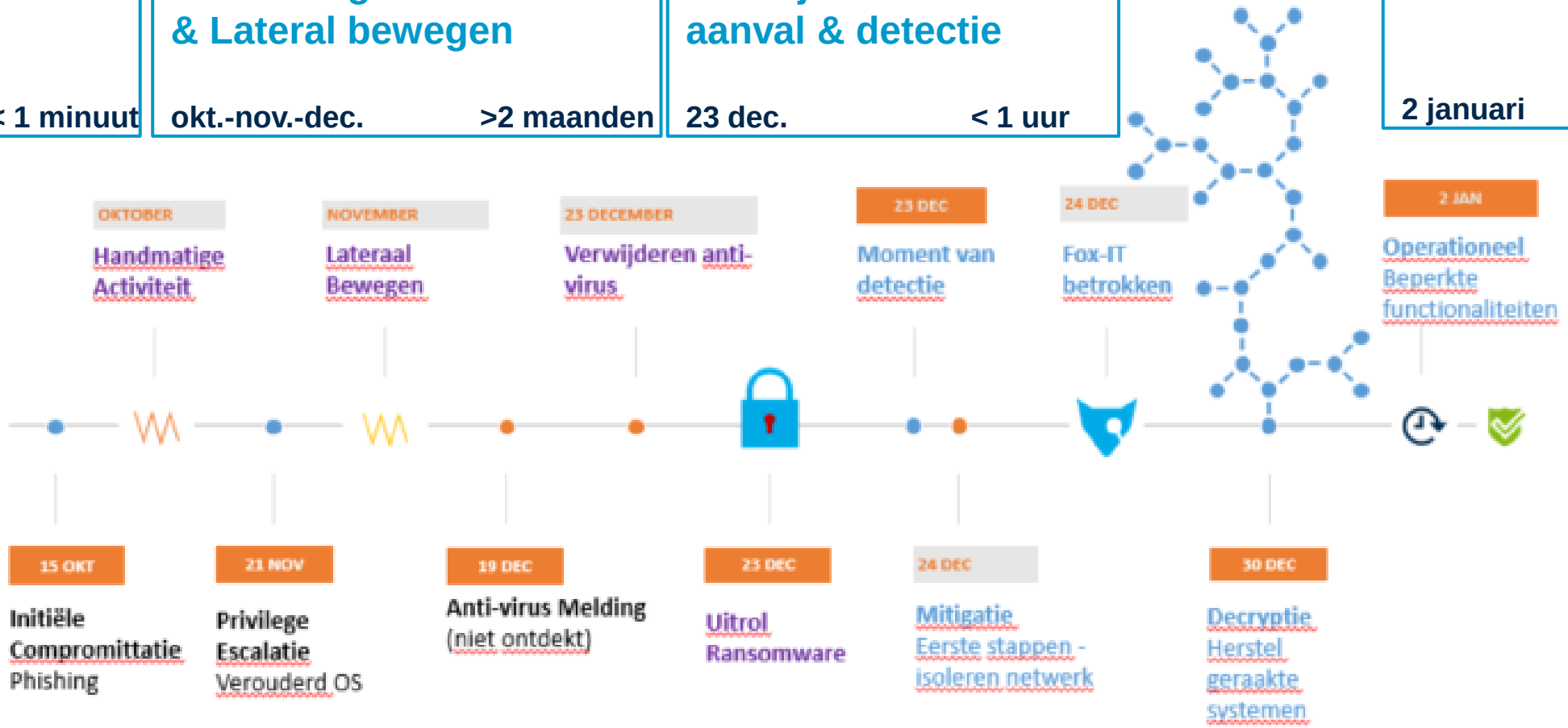
Please let me know if you have any questions

Kind Regards,

[redacted]

Tijdlijn in 3 stappen

Initiele aanval		Handmatige activiteit & Lateral bewegen		Feitelijke ransomware aanval & detectie		Deadline
15 okt.	< 1 minuut	okt.-nov.-dec.	>2 maanden	23 dec.	< 1 uur	2 januari



Crisis Management Team (CMT)

FOX-IT:

- Forensics
- Monitoring: Sensoren, Carbon Black, 24/7
- Extern geweten (naast SURFcert en NCSC)

UM:

- Inventariseren en veiligstellen systemen en data
- Herijking “basis hygiëne” van servers en backup-situatie
- Malware mitigeren en systemen opbouwen
- Aangifte en melding bij AP
- Kroonjuwelen?

->Processen en systemen/data

2 JAN

Operationeel
Beperkte functionaliteiten

30 DEC

Decryptie
Herstel geraakte systemen

Niet betalen?:
Maanden nodig voor herstel -> Gigantische kosten

Deadlines
Examens @ 6 jan. 2020 : Student Portals Live @ 2 jan. 2020

Betalen of niet betalen?

Hoe dan?

Communicatie:

- Privé email, SMS, Whatsapp, Signal (zonder mijn contacten lijst ☹)
- info@m-u.nl (met dank aan SURFnet!)
- Intern = Extern:
  - CMT, CvB, CBB, I4MU, ICTs, RvT, MT, HBO -> 200+ personen
  - En alles is WOB-baar !
    → **de UM kiest voor transparantie en besluit tot openbaarmaking** (zodra dat verantwoord is)
- Vertrouwelijke info delen? (UM/SURF/Uni's -> lekken naar "Observant" en Tweakers)
- Met de hackers……
- Updates op UM-website (werd zeer gewaardeerd)

"Mis-"communicatie:

- SURFconext (de federatieve infrastructuur, onmisbaar bij de live-gang op 2 jan)
- (Social) media: speculaties, "onzin" (neutraal tot positief sentiment)

Crisis Management Team (CMT)

24 december 2019

CMT

AVG

+ Call centre -> Stud/medew.
FG -> AP
FS -> Security
Dir. Fin -> Bitcoin service
……

Ouders !!

OCW, RvT, NWO,…

Collega CIO/CTO's

FOX-IT, Leveranciers, klanten (OU, Zuyd)

SURF, SCIPR/SCIRT, NCSC, Politie, MUMC, Hackers

Politie

Pers

Concullega's

CvB: Portefeulllehouder IT
(+ Vz. + Rector als nodig)

CIO

CTO

CISO

Dir. JZ

Dir. M&C

Woordvoerder (M&C)

FOX-IT (2 pers.)

Directeuren, Decanen (MT), U-raad, HBO

Informatie Managers

ICTS-teams

Teamleiders IT, UM-SOC (i.o)

M&C-team

Never waste a good Crisis

De eerste week

- Wachtwoord reset
- Lange wachtwoorden voor studenten (> 15 karakters)
- Geplande changes uitvoeren (we zijn nu tóch down)
- Oude tools uit en nooit meer aan
- Weesaccounts dichtzetten
- Security By (re-)Design en By Default

In de toekomst

√ Uitbreiding SOC (in januari 2020 gestart met 2 fte, nu 4 fte)

√ IB in projecten

√ Betere tools en procedures (inclusief mensen en budget)

√ Centralisatie waar nodig (beleid, audits, tools)

Lessons learned

- Awareness, awareness, awareness (management, IT-staf, gebruikers)
- Verbeteren monitoring en logging
- Incident respons en Crisismanagement
- “Offline” backups en data recovery
- CMDB
- (micro)Segmentering netwerk
- Segmentering windows domein (admin structuur)
- Security By Design en By Default
- Macro beleid heroverwegen

-> 10 projecten (MFA, awareness, (I)AM, MDM,….)

Kroonjuwelen (data)

FOX-IT rapport:

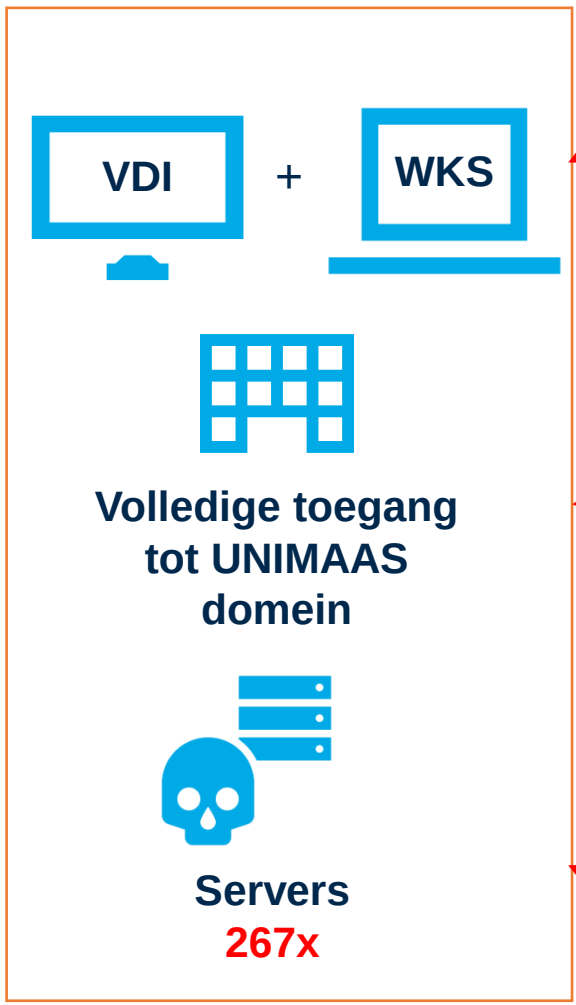
- Geen sporen van data exfiltratie anders dan de netwerk topologie en credentials
- Geen sporen aangetroffen die wijzen op het verzamelen van andersoortige data
  - Binnen de beperkte scope van het onderzoek
  - Gezien de beperkte beschikbare tijd (24 dec. tot 5 feb.)

UM (aanvullend onderzoek):

- Geen bewijs gevonden van data exfiltratie, mutatie of verwijdering

1. **Op de Studenten administratie in relatie tot de bekostiging (voorjaar 2020, forensisch)**
   - Document management applicatie (Corsa) en Fileshare met persoonlijke student bestanden
   - Bevindingen bevestigd door een externe second opinion
2. Op de Document management Database server (Corsa, zomer 2020, forensisch)
3. Op de Onderzoek data opslag (De Maastricht Studie, zomer 2020, technische risk assessment)
4. Op het Dark Web (zomer/herfst 2020, Research Project: onderzoek 12 Marketplaatsen)

Strategische lessen



Initiële aanval (15 okt)

- **Phishing** (mail op Windows Clients)
- **MS-Office Macro**: **SDBBot** malware (in Reg.)
- -> contact elke 15 minuten (als online)

Lateraal bewegen (okt/nov/dec)

- **Meterpreter** (handmatige communicatie)
- **EternalBlue exploit** (niet altijd bevestigd)
- **PowerSploit** (PowerShell-scripts)
- **PingCastle** (-> AD struktuur)
- **Mimikatz** (admin rechten op 21 nov)
- **Cobalt Strike**, Meterpreter & **AdFind** (op Domain Controller)

Uitrol ransomware aanval (23 dec)

- **sage.exe** op 3 servers (disable McAfee)
- **swaqp.exe** encrypt 267 servers (disable Windows Defender):

Wees voorbereid

- Stel een duidelijk Security beleid vast
  Security by Design & Default, 3LoD model,…
- Classificeer je processen en data
- Implementeer maatregelen

Wees geïnformeerd

- Implementeer een SOC:
  Security Operations Center
- Implementeer een SIEM system:
  Security Information & Event Management
- Organiseer samenwerking
  - Deelname Community of Practice
    bv SURF-SCIRT/SCIPR ; CIP; Netwerk-IBP
  - Uitwisseling dreiging en Kennis
    bv SURFcert/SCIRT en NCSC

Wees paraat

- Installeer een CSIRT (/CERT):
  Computer Security Incident Response Team
- Installeer een (Cyber)crisis management organisatie
- Oefen!

Was UM voorbereid?

Wees voorbereid

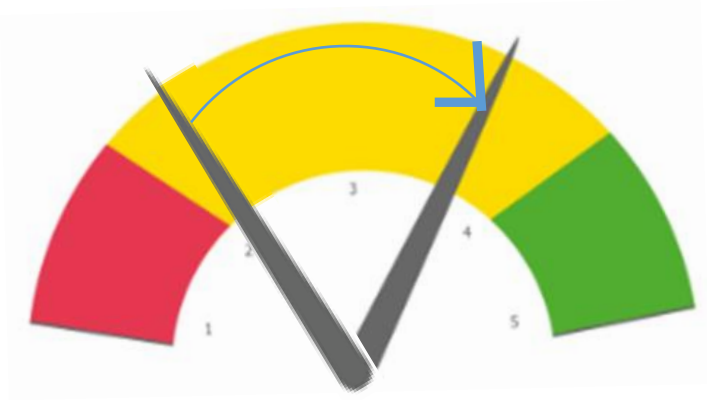
- Security beleid: By Design & Default
- Classificeer je processen en data
- Implementeer maatregelen

Wees geïnformeerd

- SOC
- SIEM
- Community of Practice

Wees paraat

- CSIRT (or CERT)
- Crisis Management Organisatie
- Oefenen !



But this was all…… *Work in Progress!*

Cybersecurity strategie 2022-2028: aan de bak!

Nieuwe Nederlandse cybersecuritystrategie (NLCS) 2022-2028:

- https://www.nctv.nl/documenten/publicaties/2022/10/10/nederlandse-cybersecuritystrategie-2022-2028

Actieplan:

- https://www.nctv.nl/documenten/publicaties/2022/10/10/actieplan-nederlandse-cybersecuritystrategie-2022-2028

➔ **pagina 15: weerbaarheid onderwijs sector**

In vogelvlucht:

- https://www.nctv.nl/documenten/publicaties/2022/10/10/nederlandse-cybersecuritystrategie-in-vogelvlucht

Pagina 15: Digitale weerbaarheid onderwijs

PO, VO, MBO, HO:

Actie samenvatting	Tijdlijn	Eigenaar
Er wordt een normenkader informatie-beveiliging en privacy geïmplementeerd voor het primair en voortgezet onder-wijs, incl. periodieke monitors en benchmarks om te volgen of schoolbesturen voldoen aan de norm.	2022-2024	OCW

Actie samenvatting	Tijdlijn	Eigenaar
Schoolbesturen in het primair en voort-gezet onderwijs besteden in hun jaarverslag verplicht expliciet aandacht aan informatiebeveiliging en privacy.	2022-2024	OCW

Actie samenvatting	Tijdlijn	Eigenaar
In het primair onderwijs, voortgezet onderwijs, MBO en hoger onderwijs wordt gewerkt aan bewustzijn van digi-tale risico's en maatregelen bij studenten, medewerkers en bestuurders door middel van campagnes, crisisoefe-ning en speciale werkgroepen.	2022-2024	OCW

+ voor MBO en HO:

Actie samenvatting	Tijdlijn	Eigenaar
De instellingen in het hoger en middel-baar beroepsonderwijs gebruiken voor hun audits het NBA volwassenheids-model en afgeleid hiervan het Toetsingskader Informatiebeveiliging Hoger Onderwijs van SURF.	2022-2024	OCW Betrokken SURF

Normenkader:

ook voor MBO en HO
-> NBA = toetsingskader, tegen gelijke normen (SURF benchmark)

Toetsingskader:

ook voor PO en VO
-> Anders wordt een benchmark lastig….

https://aanpakibp.kennisnet.nl/

Awareness !!!

ook specifiek voor IT- medewerkers.

Wat hebben we gezamenlijk ?

IBP-beleid

- Is niet wezenlijk anders

Communities

- BIC; **po/vo Netwerk-IBP**; MBO Netwerk-IBP; SCIRT ; SCIPR (met U-CISO, HBO-CISO en FG netwerken)

Awareness

- OPROEP: Het helpt ons allemaal als leerlingen ook “cyberles” krijgen ➔ aangeleerd gedrag

Oefenen

- Ozon/Nozon ➔ Doe een “lean” table-top oefening

Vendor Risk Management

- APS IT-Diensten, SIVON, MBOdigitaal, SURF

En uitdagingen……

Uitdagingen…

SOC en Crisis Management Organisatie

- 24/7 bereikbaar?
- Vrijwillig (≠ vrijblijvend) of consignatiedienst?
- Mandaten?

Backup/Restore

- On-line (snel weer in de lucht bij storingen)
  - Alleen full-restore/emergency? Of ook individuele file-restore of point-in-time restore
- Off-line (hoe snel weer in de lucht bij bv ransomware)

MFA

- Met privé middelen? Hoe ver ga je als instelling?

Thuiswerken

- Managed/unmanaged devices **-> MFA-certificaat op privéwerkplek? -> toegang tot Magister/Parnassus…?**

Audit/benchmark

- Selfassessment of (NBA)toetsingskader
- Evidence based ➔ ISMS, documentatie
- Opzet, bestaan en werking

Vragen voor jezelf(/je leveranciers)

Wat zijn mijn afspraken mbt backup?

- Kan ik (snel) een restore regelen?
- En op welk niveau? (point in time, individuele file/mailbox?)

Ik wordt gehackt, wat is de impact?

- Wat zijn de “stepping stones” (laptops, servers, netwerk?)
- Wat kunnen ze dan (via een account of malware)?
  - Lokaal admin rechten op laptops?
  - Afscherming van servers onderling?
  - Geen domein-admin over servers heen?
  - Beheerderstoegang vanuit internet zonder VPN/MFA/proxyserver?
    - Beheerdersacount ipv regulier account?
  - Welke opties heb ik voor forensics?
    - Alles traceerbaar? Toegang tot logfiles?

"Information Security is no Democracy; at best, it's a Friendly Dictatorship"

Based on: Jaya Baloo