Cyber-attack: the day after (and much longer)

Ivo Jacobs
Managing Director, H.H. Hospital of Mol
What happened?
Tuesday, February 2, 2021

Start IT employee & performance issues 7:15
Performance issues

- Zabbix – management console – IT department
  Performance indicator → slowdown of systems

- Unusual activity from DC (domain controller)
  (scripts → account disabled)
Tuesday, February 2, 2021

Start IT employee & performance issues

7:15

Performance issues confirmed

8:00

Ransomware found
Performance issues confirmed

- All activity halted
- Word message on some PCs

Ransomware found

- EPD not corrupted
- Disabling internet, intranet, programs, internal/external email traffic...
- Isolate backup files
Tuesday, February 2, 2021

Start IT employee & performance issues

7:15

Performance issues confirmed

8:00

Ransomware found

9:00

Crisis cell (management, nurses, doctors...): impact?
Crisis cell (management, nurses, doctors...): impact?

- Activate internal disaster plan (emergency procedures – business continuity)
- Activate insurance (cyber insurance)
- Contact CERT – police government
- Intake & study environment → Install recovery plan → Contact external IT experts (insurance)
  - Isolate all (possibly) infected systems
  - Complete IT shutdown
Crisis cell impact

Communication
- Internal: WhatsApp pyramid
  → Emergency measures – patients present
  Cave: conflict IT security vs patient security
  Who’s in charge?

- External → partners, government, ZNI
  Via secure internet connection

Conflict
- IT department: shut down everything immediately
- Doctors/nurses: keep access open to consult essential data of patients present

→ Who has ‘the lead’?
Tuesday, February 2, 2021

Start IT employee & performance issues at 7:15

- Performance issues confirmed at 8:00
- Ransomware found at 8:00

Crisis cell (management, nurses, doctors...): impact? at 9:00

- External IT experts at 16:00
- Start recovery at 16:00
External IT experts

- Objectives
  - Define corrupted systems (50 out of > 800)
  - Define ransomware type
  - Define backup and recovery options
  - Define repair priority systems
- IT crisis team: analysis of technical solutions
  - Operational crisis cell → business continuity plan
  - Doctors, nurses, administration, reception...
  - Planning, data collection, reception, contacts
Start recovery plan (externe IT experts)

- Dividing infected / non-infected systems – isolation
- Re-installation & cleaning: ‘Wash street’
- Install comprehensive antivirus software
  Uninstall antivirus hospital – new software
- Start installing backup data

Contact with the attackers
The next days

Negotiating with the 'attackers': IT experts + insurance

- Ethical aspects!
- Costs of damage - recovery  ▪ Who has ‘the lead’?
- Threat to patient safety?

‘Business model’ cybercriminals:

- Promises
- Safety issues
- Credibility
  ▪ Honest deceivers
- Data leakage?
Hi,

It looks like you have encrypted our systems. We are a Belgium Hospital. Our patients are in serious danger. Can you provide us the decryption key please, so we can start recovering our environment?

Our UUID is: 0f5cbf7b-741d-4576-9a8d-b71628a7acef2f
Hi,

It looks like you have encrypted our systems. We are a Belgium Hospital. Our patients are in serious danger. Can you provide us the decryption key please, so we can start recovering our environment?

Our UUID is: 0f5cbf7b-741d-4576-9a8d-b71628a7acef2f

Hello, if you want to decrypt all files, you need to pay BTC.
Hi,

It looks like you have encrypted our systems. We are a Belgium Hospital. Our patients are in serious danger. Can you provide us the decryption key please, so we can start recovering our environment?

Our UUID is: 0f5cbf7b-741d-4576-9a8d-b71628a7acef2f

Hello, if you want to decrypt all files, you need to pay BTC.

Do you understand that you encrypted the network of a hospital? Lives of people could be at stake. I urge you to provide the decryptor for free and as soon as possible, so the impact is minimum.
Hi,

It looks like you have encrypted our systems. We are a Belgium Hospital. Our patients are in serious danger. Can you provide us the decryption key please, so we can start recovering our environment?

Our UUID is: 0f5cbf7b-741d-4576-9a8d-b71628a7acef2f

Hello, if you want to decrypt all files, you need to pay 1 BTC.

Do you understand that you encrypted the network of a hospital? Lives of people could be at stake. I urge you to provide the decryptor for free and as soon as possible, so the impact is minimum.

If you don’t want to pay, please don’t bother me.
Hi,

It looks like you have encrypted our systems. We are a Belgium Hospital. Our patients are in serious danger. Can you provide us the decryption key please, so we can start recovering our environment?

Our UUID is: 0f5cbf7b-741d-4576-9a8d-b71628a7acef2f

Hello, if you want to decrypt all files, you need to pay 1 BTC.

Do you understand that you encrypted the network of a hospital? Lives of people could be at stake. I urge you to provide the decryptor for free and as soon as possible, so the impact is minimum.

If you don’t want to pay, please don’t bother me.

Ok, let me discuss this with the board of the Hospital.
Conclusion

- They’re polite boys those hackers.
- You can’t negotiate with them.

UNLESS....

- A reduction in the requested ransom
- Desinterest
### The next days

<table>
<thead>
<tr>
<th>Root cause analysis</th>
<th>Problem: service account suppliers &amp; remote support</th>
<th>External communication problem</th>
<th>Execute recovery plan (ctd)</th>
</tr>
</thead>
</table>
| • Hacking website (Sharepoint) → access via old DC account system-level |  | • What happened  
• Impact inside  
• Impact on patients  
• What did we do to recover?  
• Timing of recovery?  | • Reinstall all connections  
• New username and password policy  
• ‘big bang’ (paper!)…  
• 2 Factor Authentication |

- [Hacking website (Sharepoint)]
- [access via old DC account system-level]
Lessons learned
Lessons learned

Organization
- Information Security Management System (PDCA cycle) – ISO27001 of NEN7510
- Invest in IT-team (training in cybersecurity and recovery)
- Physical security organization (access control)
- Business Continuity Plan
- Procedure Cyber Insurance – be ready for ‘CERT’ (network description)

Policy
- Policy (clean-desk, accurate password policy, incident readiness,…)

Behavior
- Awareness
Lessons learned

Technical
- Rebuild website
- Invest in security monitoring, detection and response
- Office 365 migration
- MFA (multi factor authentication)
- Clean Active directory & remote support & service (SilverFort)
- Vulnerabilities and patches
- Network segmentation
- Network access control (802.1x)

- Backup & recovery (importance of off-line backup)
- Clean up IAM (i.e. after resignation)
- Improve workstation security (Anti virus next level - EDR solution)
- Forensic readiness (control logs)
- Backup internet line and telephone
- (RDP – Citrix – Office macro’s - )
A word about the cost of an attack...

Direct costs

- IT Experts – €450/hour…
  5 days, 12 hours/day, 4 people + remote… → Total cost of 180K
- Own (human) resources (MDs, secretary, reception…)
- Additional software/hardware

Indirect costs

- Immediate damage costs: stop medical activities (e.g. all examinations, operations,…)
- Future damage costs: missed future appointments
- Loss of information (lost billings,…?)
- Restore missed information
- Reputation damage
- Medical damage?
- What if questions (data leakage, …)
→ Total cost estimated 700 – 1,000 K
We no longer have an insurance...

- Immediate cancellation existing insurance
- Need to define damage claim before new proposal
- No other insurance company ‘willing’
- Conditions (you can’t refuse)...
- External supervision/control

Outsource IT?
Time for a Zero Trust approach
Zero Trust: a new reality needs new principles

Verify explicitly

Use least privileged access

Assume breach
Zero Trust set-up H.H. Mol
Why SOC as-a-service?

- **Unburdening**: cybersecurity follow-up is complex: specialized knowledge & resources required
- **Follow-up is necessary**
  - Proactive
    - Insights from SOC form the basis for evolutionary improvement actions, both through technological evolution and from SecOps.
  - Reactive
    - Suspicious incidents are not always resolved 'automatically' by the technology; manual follow-up and intervention are necessary. Being agile is very important in cybersecurity.
- **SOC is often a prerequisite for (affordable) cybersecurity insurance**
Azure AD Conditional Access + Identity Protection

**Conditions**
- Employee & Partner Users and Roles
- Trusted & Compliant Devices
- Physical & Virtual Location
- Client apps & Auth Method

**Controls**
- Allow/block access
- Limited access
- Require MFA
- Force password reset
- Block legacy authentication

**Policies**
- Machine learning
- Real time Evaluation Engine
- Session Risk
- Effective policy

**Geo-location**
- Corporate Network
- Browser apps
- Client apps

**Device Types**
- Android
- iOS
- MacOS
- Windows
- Microsoft Defender for endpoints

**Cloud SaaS apps**
- Microsoft Cloud
- On-premises & web apps

**Microsoft Cloud App Security**
General conclusion
General conclusion
General conclusion
Take home message

By failing to prepare, you are preparing to fail.

~ Benjamin Franklin
Take home message

By failing to prepare, you are preparing to fail.

~ Benjamin Franklin

For every level there's another Devil.

~ Tyrone Gibson
Take home message

By failing to prepare, you are preparing to fail.

~ Benjamin Franklin

For every level there's another Devil.

Tyrese Gibson
Take home message

By failing to prepare, you are preparing to fail.

~ Benjamin Franklin
Take home message

By failing to prepare, you are preparing to fail.

~ Benjamin Franklin
Thank you