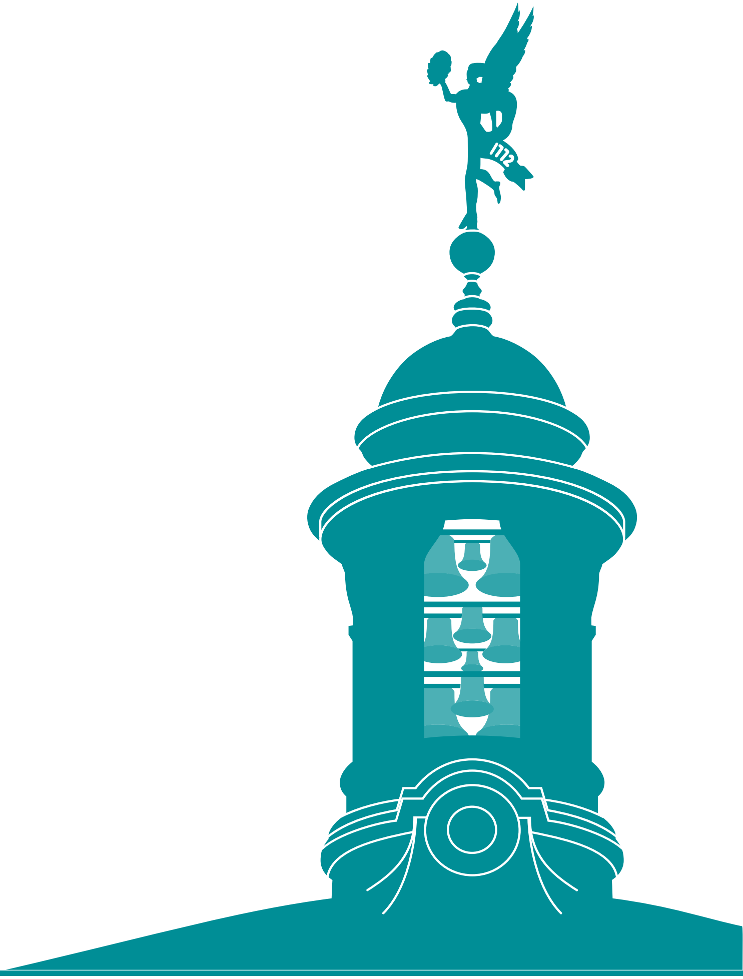
WWU
MÜNSTER

Cyber security threats and how to deal with them

Raimund Vogl

Center for IT, University of Münster, Germany

rvogl@uni-muenster.de



The Threat Situation

- Cyberthreats known for long – The Internet Worm – 1988
- Carnegie Mellon University (CMU) to found first Computer Emergency Response Team (CERT™) in 1988
  - Only few other HE institutions with early CERTs (Münster approx 2000)
- Evolution: Viruses, Malware, D(D)oS attacks, botnets – limited impact
- Mid 2010‘s: crypto malware – ransomware
- Late 2010‘s: cyber criminal „franchises“ launching coordinated attacks – massive impact on business operation

Who is attacking – and why?

- High diversity
  - Activists – white or grey hat
  - State actors (espionage, cyber warfare) – Advanced Persistent Threats ATPs
  - Criminal organisations (e.g. HIVE, Lockbit, Vice Society) -> some focus on HE

How do they attack?

- Systems vulnerabilities („exploits“):
  - From outside or from local user; unprivileged user gain administrator rights
    - Start with unprivileged compromised accounts (phishing, darknet shops)
    - Search for exploits, potentially wait for months till successful
    - When gained admin access, move on to other systems (lateral movement).
    - Active Directory makes complete takeover easy once compromised
  - Zero-Day exploits (rare) vs. known exploits (fixes/patches exist)
  - Basically all successful cyber attacks used unfixed know exploits: IT-admin flaws!

How do they attack?

- Once takeover has happened, these steps are executed:
  - finding the backup systems and destroying the backups (if they are also part of the active directory, this is an easy step)
  - exfiltrate data for later blackmailing (institution or its customers)
  - role out encryption scripts that can be started on all systems in the AD simultaneously.
  - After encryption has been performed, criminals usually leave behind message files on how to get into contact with them for ransom payments.
- Sometimes breach discovered before encryption started – act fast!

What to do against cyber attacks?

- A CIOs take on things – managerial bullet points, not technical
    - my own lessons learned and to remember
- Münster University‘s actions starting July 2022 (after attack on FH Münster)
- Based on analysis of attacks on other HE institutions and workshops with cyber security consultancy

What to do against cyber attacks? 1/2

- Select and engage a cyber security consultancy before anything happens
- Foster user awareness for cyber security
- Establish high professional standards for IT administration
- Secure system administrator access
- Identifying server systems and classifying their protection needs
- State of the art firewalling (NGFW)
- State of the art anti-virus software
- Central logging - Security Information and Event Management (SIEM)

What to do against cyber attacks? 2/2

- Mandatory multifactor authentication for all users when accessing from outside campus network
- Securing the Windows Active Directory (AD) – and segregating Backup, vSphere, Storage Administration from general AD
- Fortify the backup systems – your last resort
- Have emergency plans and procedures ready and prepare necessary tools
- Prepare to rebuild infrastructure from scratch out of backups – “black start”

What to do against cyber attacks? Emergency Plans

- Have procedures and relevant contact data ready on paper or locally on your personal devices as standalone files (PDF)
- Procedure to disconnect from the internet (when breach/imminent encryption is detected).
- Procedures to shutdown central systems (to stop already running encryption).
- Communication the top management that the cyber-attack emergency happened
- Establish tools for secure access channels from outside
- Establish and periodically test tools for emergency communication amongst the IT experts
- Prepare communication to end users: e. g. through an externally hosted web presence with prepared basic emergency information (dark site)

Conclusion and Outlook

- Considerable own effort needed
- Operative IT security measures as described – and accompaning organisational measures – Information Security Management System (ISO 27.001, BSI IT-Grundschutz)
- Being better prepared than many others is key (you don‘t have to run faster than the bear …)
- Ransomware is a customer focussed business – customers not willing / being able to pay will let it come to a halt – so we may hope

Thank you for your attention

Contact: rvogl@uni-muenster.de