EPiC Series in Computing
Volume 95, 2023, Pages 285–290
Proceedings of European University Information Systems Congress 2023

Cyber security threats and how to deal with them

Raimund Vogl[1*]
[1] WWU IT, Westfälische Wilhelms-Universität Münster, Germany
rvogl@uni-muenster.de

Abstract

Information security and cyber threats have been among the top concerns of IT managers for many years. But recently, the level of threat has grown considerably and has reached a new dimension with companies being severely impacted by cyber-attacks, even being driven into bankruptcy. This is also affecting higher education institutions, with several universities spectacularly falling victim to ransomware attacks. For IT managers, it is now crucial to react to this threat, strengthen their cyber defense and also prepare to mitigate successful attacks. We describe the measures Münster university has recently implemented in a massive effort to prepare for the common types of attacks. This is meant to be an IT manager focused semi-technical overview on the topic of threats and remedies to help evaluate the own situation and evaluate possible measures.

1 The threat situation

Cyber threats have been around almost as long as (networked) computers exist. At Münster university, a CERT (Computer Emergency Response Team) has been established since the early 2000’s to deal with cyber security incidents. Until the early 2010’s, these incidents mainly used to be individual computers being infected by malware, potentially being abused for spam emailing (and, of course, users doing copyright infringements etc…). With new types of malware, botnets became a more widespread phenomenon, and (distributed) denial of service attacks became a widely felt nuisance, which luckily today can fairly well be mitigated by internet providers and usually no longer bothers us. Crypto malware became a real concern in the mid 2010’s, with names like WannaCry, CryptoLock, Emotet and ryuk gaining infamous reputation. These malware programs usually entered through email or web downloads and could affect individual personal computers or shared network drives – a risk with limited impact where recovery from backups is usually possible limiting the damage, and ransom demands are of moderate size.

But in the late 2010’s, a completely new situation arose, with criminal organizations deliberately attacking companies or public institutions, taking over their central IT infrastructure to exfiltrate (steal) sensible data for blackmailing (the victim institution and potentially those referenced in the data) and

[*] https://orcid.org/0000-0002-6681-1530

then encrypting data and systems for ransom. This is no longer of limited impact, since a key part of the attack is to destroy the backup systems, and ransom demands for the victim institutions are – tailored to their financial capabilities – in the range of hundreds of thousands to millions of Euros.

When companies are victim to cyber-attacks, they usually try to keep this secret and information on the attacks and their circumstances are rarely disclosed – only in cases of business partners being effected or in the case of a subsequent bankruptcy limited information is released. Since universities are more open and have no means to impose secrecy on their students and employees, such events are best documented for higher education and research.[†]

Amongst IT managers and information security experts at German universities, there is extensive exchange on the incidents that have recently happened. This gives some insight into how the cyber criminals execute their attacks, and what the aftermath for the victim looks like.

These dire prospects prompted WWU IT, the central IT provider for Westfälische Wilhelms-Universität (WWU) Münster, to strongly focus on strengthening IT security measures starting from mid-2022, additionally triggered by attacks on several nearby universities.

2 Who is attacking, and why

There is a listing of hacker groups on Wikipedia[‡], which gives an impression of the diversity of these groups. Some are actors with ideological motives (e. g. Anonymous), some are state actors (sometimes also called Advanced Persistent Threats (APT) – such as the Russian cyber-espionage group Fancy Bear or APT28), and some are effectively operating criminal organizations. The two that are currently best known, are not even in the Wikipedia list. One of them is HIVE, that was said to be number two in that market, which was recently taken down by internationally coordinated police action.[§] Another one, that is said to be responsible for one third to half of the ransom attacks, is Lockbit.[**] This is a startup-like organized enterprise with an estimated 3-digit "employees" and an estimated "revenue" of 100 million Euros since its formation in 2019.

Universities should expect to be targeted by one of these strictly financially focused criminal organizations. One other such group is Vice Society, which seems to be targeting universities with priority – their "customers" or "partners" are featured on their darknet site (accessible with TOR)[††] where, in case of not compliance with ransomware demands, the routinely exfiltrated sensible data is disclosed.

3 How do they attack

There are software vulnerabilities that can be exploited to directly gain privileged access to systems (even from outside the campus network, if those systems are exposed to the internet), but these are rather rare and made public readily after their discovery (to name just two examples: the "shitrix" exploit in Citrix ADC/Netscaler and the log4j/shell4j exploit) so that system administrators can deactivate compromised services (to overcome the "zero day" phase while vulnerabilities are known and tools to exploit them are available but no fixes/patches are yet available) and apply patches that are hopefully soon available. Minimizing the number of systems and software products exposed to direct

[†] https://konbriefing.com/de-topics/cyber-angriffe-universitaeten.html (in German)

[‡] https://en.wikipedia.org/wiki/List_of_hacker_groups

[§] https://www.nationalcrimeagency.gov.uk/news/hive-takedown-nca-in-international-operation-to-shut-down-100m-ransomware-threat

[**] Frankfurter Allgemeine Zeitung, March 4, 2023, page 24 (in German)

[††] http://vsociethok6sbprvevl4dlwbqrzyhxcxaqpvcqt5belwvsuxaxsutyad.onion/

access from the internet obviously helps reduce this threat. And cyber criminals are not reported to utilize previously unknown exploits (this is rather the domain of state actors for cyber espionage, who rarely target higher education institutions). But this emphasizes the importance of proper systems administration to immediately fix such vulnerabilities as soon as they become known – sadly, many successful cyber attacks are due to known exploits that have negligently been left unpatched.

From all cyber attack incidents we are aware of, the attackers found access to systems on the campus network from outside through compromised (unprivileged) user credentials. Steeling credential usually happens through phishing – fake emails directing users to websites that are prompting them to enter their credentials. These stolen credentials are traded (by the “phishers”) on the darknet, and ransomware attackers seem to come back to offerings when resources are available for new engagements. Thus, stolen credentials can be put to use long (reportedly even several years) after they were obtained. Incidentally, we noticed that these stolen credentials even seem to be regularly checked upon and maintained – with the role out of multifactor authentication, we were informed by several users that someone else activated multifactor for their accounts – making it clear that criminals were trying to save their assets.

Using such ordinary (unprivileged) user accounts, attackers start to explore the opportunities and try to gain access to other systems (lateral movement), always scouting for vulnerabilities (missing patches, or loose administration practices in using privileged credentials) that could be exploited to gain privileged access. It is usually Microsoft Windows Server systems and Active Directory (AD) domain controllers which are in the focus of the attackers (e. g. using tools like Mimikatz[‡‡] to read out cached administrator credentials). Once privileged access to the Windows AD was obtained, the next steps usually involve a) finding the backup systems and destroying the backups (if they are also part of the active directory, this is an easy step), b) exfiltrate data for later blackmailing, c) 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.

In several cases known to us, the criminal activities were discovered in the late stages of preparation – just before the encryption scripts could be launched. In such situations, immediate action is required to cut of the campus network from the internet and thus severing the criminals access.

It should be noted, that not only Windows AD can be a target for hackers – there is also cases where they infiltrate unix/linux systems (which was the case in the well know early 2020 attack on European HPC centers[§§]), VMware hypervisors and vSphere management platforms, or storage and backup systems (like Spectrum Scale or VEEAM).

4 What to do against cyber attacks

Drawing from the experiences with the concerted effort to strengthen IT security measures at WWU IT, we want to point out these measures as essential to prevent a cyber-attack from causing havoc for an institution:

1. <u>Select and engage a cyber security consultancy before anything happens:</u> to try and find a source of support when the worst has already happened is not a good way to go. Cyber-attacks are so common, that proactively contracting a well-chosen consultancy is almost indispensable. They usually help to analyze the level of preparedness of their customers (in workshops, giving

[‡‡] https://de.wikipedia.org/wiki/Mimikatz

[§§] https://www.bleepingcomputer.com/news/security/european-supercomputers-hacked-in-mysterious-cyberattacks/

valuable input to improve your security measures) and are available with a hotline and emergency team in case of an attack.

2. Foster user awareness for cyber security: compromised user accounts are the origin of almost all attacks (vulnerabilities of systems that allow privileged access from outside without first having a local unprivileged account are very rare). So preventing users from being tricked by phishing emails or websites is key. Regular drills with simulated phishing attacks can help to gauge the awareness level.

3. Establish high professional standards for IT administration: security advisories by systems/software suppliers and official agencies must be immediately followed. It has to be made sure that the latest (security) patches are applied on all systems. Estimates go that 80% of incidents are due to open (known) vulnerabilities (missing patches) – the other 20% to user errors (phishing, improper handling of privileged credentials).

4. Secure system administrator access: multifactor tokens have to be mandatory for system administrators. Administrators have to strictly separate their personal account from the administrator privileges. Windows (AD domain) administration must only be allowed from dedicated machines. Administrator remote access must go through dedicated jump-hosts with multifactor authentication.

5. Identifying server systems and classifying their protection needs: central IT has to be aware of all “server” systems in the campus network – and the level of protection required by the data stored on these systems.

6. State of the art firewalling: in the good old days, it was customary for universities to have all IT systems directly connected to the internet, allowing them to function as worldwide accessible servers; only subsets of systems with higher protection needs were explicitly blocked by firewall rules (blacklisting). This very liberal policy is still in practice in several universities. Due to the rising threat level, it is indispensable to reverse this policy to only exposing selected systems to access from the internet (whitelisting), and keeping their number small. Current next generation firewall (NGFW) systems do not only block address ranges, but are able to deeply inspect the ongoing traffic, noticing and blocking suspicious activities (file signatures for web malware and address lists of suspicious sites are continuously updated and can be blocked). Using them to block e. g. the TOR protocol from server networks is a good step, since this is often used by attackers for obfuscated communication. NGFW can be supported by secure web proxies (allowing to inspect also the otherwise intransparent encrypted ssl communication that has become standard on the web) and Mail/Spam-filtering appliances.

7. State of the art anti-virus software: standalone anti-virus software is no longer sufficient – cloud-based solutions gathering and consolidating threat intelligence from all institutional systems, allowing to have early warning of rising threat levels, are the standard to adopt.

8. Central logging: to be able to gain intelligence on suspicious activities distributed over several systems, it is mandatory to consolidate log information (on a sufficiently detailed level, including all security relevant events like logins and privileged operations) in a central logging facility. Storing data over an extended period of time (usually 90 days, potentially more; since this is also a data privacy issue, it is good to store these log data on a well secured location with highly restricted access) also helps for forensic investigations, and also to understand what systems have been affected by hacker activities and need to be newly set up. This is usually referred to as Security Information and Event Management (SIEM), especially when the aggregated data is also used for real-time analysis and alerting. Such security operations are also provided as services by various suppliers.

9. Mandatory multifactor authentication for all users when accessing from outside campus network: the common attack vector is compromised user accounts, giving attackers from the internet access to systems in the campus network from where they can scout form exploits. To close this, it is necessary to invalidate stolen credentials by mandatory multifactor authentication for all access from outside the campus network - via VPN, accessing VDI virtual machines, accessing Remote desktop servers. All web applications requiring login should be accessible only from the campus internal network (after VPN connection or from remote desktop servers etc…). OTP (one time password) provides a solution that can easily be established for all users, even in large communities like a university with 60.000 users. It integrates nicely with VPN Clients, VDIs and several web-based software systems. A portal that allows users to do self service of their MFA settings is mandatory here, which itself requires MFA protection. Ultimately, MFA only makes sense when it is not optional but compulsory for all users – otherwise criminals can activate MFA for stolen user accounts with the users themselves potentially not noticing.

10. Securing the Windows Active Directory: since the Windows Active Directory is the predominant target for attacks, it needs to be closely monitored for suspicious activities and potential configuration errors – commercial and freeware tools are available for this[***]. And on the other hand, important infrastructures like VMware ESX/vSphere, Backup-Systems, network management, etc… should be kept completely separated from Windows AD with their own administration accounts (even if this inconvenient), to prevent attacks from spreading to these assets.

11. Fortify the backup systems: since backup systems are the first target of attackers to destroy this last resort, it is indispensable to separate them as good as possible from the remaining campus systems, with separate administrator accounts and firewalling rules to restrict access other than needed for backups.

12. Have emergency plans and procedures ready and prepare necessary tools:

    a. Have procedures and relevant contact data ready on paper or locally on your personal devices as standalone files (PDF)

    b. Procedure to disconnect from the internet (when breach/imminent encryption is detected). Low threshold decision making is required

    c. Procedures to shutdown central systems (to stop already running encryption). Low threshold decision making is required.

    d. Communication the top management that the cyber-attack emergency happened and the cut off/shutdown procedures were activated

    e. Establish tools for secure access channels from outside (secured DSL entry points with jump host; a dedicated out of band communication channel to core infrastructure)

    f. Establish and periodically test tools for emergency communication amongst the IT experts (e. g. via externally hosted groupware or group chat)

    g. Prepare communication to end users: e. g. through an externally hosted web presence with prepared basic emergency information (dark site)

13. Prepare to rebuild infrastructure from scratch out of backups: have “black start” infrastructure ready as a platform to reinstall your infrastructure in case an attack happened and you have to

[***] See e. g. https://www.semperis.com/resources/2022-purple-knight-report/

restore everything from backups – or also in the case of discovering an imminent attack on time, a complete reinstall is often needed for a clean restart since it is unclear to what extend systems are compromised by hacker activities. This has to be strictly separated from the common IT environment, so that it cannot be compromised by a successful attack and is available to have a fast recovery. A separated dedicated network infrastructure with a separated internet access (e. g. a DSL-line) is advisably for situations where the main internet connection had to be severed to interrupt hacker activity.

5 Conclusion and Outlook

For universities, the threat of a purely ransom focused cyber attack is the predominant cyber-attack scenario. Observing the proposed measures should help to minimize the risk, but requires substantial efforts and possibly investments. Establishing formal information security management systems (ISMS) according to frameworks like BSI IT-Grundschutz helps to sustainably implement information security into the organization, mostly via guidelines for operations of networks, IT system management and handling of security incidents.

As to the future of this currently predominant cyber threat, we can hope that heightened security awareness and implementation of the described security measures on the one hand, and the defiance of institutions to comply with criminals demands to make payments (and, additionally, the dwindling possibilities to make the required bitcoin payments at all) will render this business less and less lucrative and attractive and will ultimately lead to its extinction.