Summary of the Information Security workshop on Ransomware, 9 June 2020

Organised by the EUNIS InfoSec SIG as a part of the EUNIS Virtual Congress 2020

PART 1 The Attacks

Bart van den Heuvel, of Maastricht University, highlights aspects of the actual CLOP\(^1\) attack. Maastricht is using Office 365, and the attack used phishing emails to get in. Immediate response was to trace phishing mails, block phishing URLs and attachments, and build a stronger firewall to keep hosting/providers of such URLs out.

To prevent spam and phishing, awareness must be raised. This is extremely important but at the same time never enough. Awareness needs to be addressed at the level of 1) management, 2) administrators and 3) user level. Don’t forget: the crisis can begin with just one person clicking on the wrong email attachment. We have to be prepared! Management awareness can best be approached by posing the question "Can we be hit?".

A HEI should have a Crisis Management in place as well as an Emergency Plan. An Incident Response Team is essential. It is important to be transparent, eliminate the rumours and replace those with clarity. Ensure that an active community deals with and communicates about these matters. Outside communications should be done by the PR department. Of course, one should learn from the crisis, try to set the priorities: "Never waste a good crisis!".

Maastricht hired professional help from outside (IT security service provider Fox-IT) and chose to be open about the attack and demonstrate to the public they were ‘doing the right thing’, informing and warning others. It was a serious attack with online backups appearing to be compromised as well.

Measures taken to avoid an attack are the new password policy >15 char; implementation of the Microsoft AD Tier concept, and segmentation and detection of lateral movement.

Tools used by attackers, among others were Ping Castle (AD structure) and Carbon Black Software.

Marius Mertens of Duisburg-Essen University informed about a very quickly discovered Emotet attack. Emotet can use a variety of ways to take control of servers. Within two hours after the first email message with previously exfiltrated data was found, action was taken to investigate and take measures. It took a day before it was clear that it was a reportable incident and six days later things were perceived to be under control (5 infected PCs found).

\(^1\)https://malpedia.caad.fkie.fraunhofer.de/details/win.clop
Marius addresses the symptoms and indicators of compromise, a list of actions taken, partners involved in solving the issue, as well as how as a result stronger awareness and stricter measures are applied such as an email signing campaign (digital certificates for certain management user), planned blocking of legacy office attachments; phishing warning and Information on the incident, etc. In the end the whole computing configuration was built up anew, and all infected machines wiped, cleared and restored with the stricter measures mentioned above.

Some technical questions were asked and discussed. Discussion addressed the fact that because of Maastricht’s open approach, there has been no reputation damage. The opposite seems to be the case: the response to solve the issue and be transparent about it added to the image of Maastricht University as a responsible organisation. The fact that this attack happened had a positive effect on security being perceived as important (and worthwhile to provide budget for). At Duisburg-Essen University this type of positive impact did not happen. The damage was too little, and the attack addressed so quickly that it did not affect budgets and staff discussions.

PART 2 Prevent & Respond as Individual HEI and in National Collaboration

The workshop continued with Remco Poortinga of SURF, explaining the role of SURF (the collaborative organisation for ICT in Dutch education and research) at national level re security issues in general. In the case of Maastricht being attacked, SURF assisted in three ways: offer support; Collate & verify information, disseminate; Check for possible problems at other institutions (via net flow data and email filter logs).

The actual attack made the national news, was discussed in parliament, and established a notion that this is organised crime, and those who are hit victims rather than guilty of neglecting security. Security was higher on the agenda and stimulated forming/strengthening of a national SOC for 24/7 Security Incident and Event Management (SIEM), use case management and advice, knowledge/information sharing and vulnerability scanning.

Marius Mertens, in the second part of his presentation pointed at various lessons learned and things that can go wrong, as well as technical and organisational recommendations. In his outlook to the future Marius predicts that we’re only at the beginning, as sophisticated attack become cheaper, stolen credentials are worth money (Bitcoins), and IoT and smartphones are increasingly offering opportunity to attack. The good news though – and bottom line lesson: All attacks discussed today can be countered by simple standard measures. They just need to be implemented.

Discussion afterwards identified that in several countries SOC have started to develop. One of the security challenged issues these all have to engage with is the devices staff and students bring in – an issue that is even more relevant in Corona-times with everyone working from home, often using their own device. This may be a future topic to discuss: Security issues around Bring Your Own Device at Higher Education Institutions (BYOD@HEI).
Discussion issues in breakout rooms:

- Awareness
- Monitoring
- SIEM, AI (expensive, staff resources)
- Increase in reporting of phishing emails
- Exchange of indicators (IOC/IOA) through MISP (https://www.misp-project.org/)
- CLAW Cyber Security Training
  https://www.geant.org/People/Community_Programme/workshops/Pages/CLAW-returns.aspx

- Individual approach:
  o Crisis communication servers at different locations (email, web, files)
  o No single measure that saves everything
  o Multi factor authentication (MFA): https://tiqr.org

- Collaborative/national approach:
  o MISP
  o Cloud Services (?)
  o Communication about ongoing attacks (share information)
  o Centralize expertise where possible
  o Checks of information important, not just forwarding
  o Expertise hard to find
  o Networking of local CERTs