Response of Maastricht University to FOX-IT report

05-02-2020

Introduction

Maastricht University became the victim of an attack by cyber criminals on 23 December 2019. In the early night of 24 December 2019, Maastricht University contacted Fox-IT BV. From that day onwards, Fox-IT provided support in the area of crisis management, mapping the circumstances of the attack, as well as forensic investigation and advice in the recovery process of the systems.

On 5 February 2020, Fox-IT delivered the report *Project Fontana*, the name the company gave to the investigation.

It concerns the factual representation of findings and recommendations based on a forensic investigation of the technical landscape.

Facts, however, always have a context. Maastricht University therefore looks at the cyber attack not only from a technical point of view, but also from the context of its own organisation. In our view, this is necessary in order to obtain as complete an answer as possible to the question of whether the university has adequately armed itself against digital vulnerabilities.

That is why the university has added to, explained or commented on a number of findings and recommendations in the report, without wanting to detract from the facts. And where UM itself is still looking for (additional) answers to specific questions on some points, (internal) research will have to provide more clarity about this in the near future.

By publishing the report, this response and the results of follow-up research, Maastricht University wants to play its part in increasing digital security.

In the increasingly intensive fight against cyber insecurity, UM regards this as its social duty.

Ransomware attack

Since the cyber attack on 23 December 2019, UM has been working hard: on the one hand, to repair the damage and, on the other hand, to make education and research possible again as soon as possible. This was the absolute commitment and focus of the Crisis Management Team (CMT), which UM immediately set up. In the course of time, the work of the CMT has shifted from removing the direct disruptions to rebuilding the services to students, academic staff and support staff. This process has been reported openly, transparently and in as much detail as possible via the (daily) updates on the university's website.

Part of our technical infrastructure was affected during the attack. That infrastructure consists of 1,647 Linux and Windows servers and 7,307 workstations. The attack ultimately focused on 267 servers of the Windows domain. The attacker focused on encrypting data files in the Windows domain. The backup of a limited number of systems was also affected.

Conclusion and follow-up

Maastricht University is confident in Fox-IT's report. On the basis of forensic research, it indicates how cyber criminals have taken some of UM's data hostage. However, in view of the scope and duration of the investigation, an in-depth investigation is both sensible and necessary. Not everything has been precisely investigated yet. UM has therefore launched an internal investigation.

On the basis of the current recommendations from the report and future findings from its own internal investigation, UM can review its security policy and determine which existing plans need to be adjusted and/or expanded.

Lessons learnt

On the basis of the Fox-IT report, supplemented with its own insights, UM can already indicate a number of 'lessons learned'. These lessons relate to cyber security in general and the December cyber attack in particular:

1. Better awareness and handling of (reports of) 'phishing' emails

We know from research that about 20% of users open so-called 'phishing emails'. By focusing more on 'awareness campaigns', the university wants to reduce the number of successful malicious attempts to attack. As soon as a 'phishing e-mail' is received by users, we want them to report it to the Service Desk. We want to use training and tools to improve the ability of the employees of this desk to take the right actions.

Thanks to internal research, we now know that with this specific attack that several variants of 'phishing mails' have been sent and that some reports of these mails have been received by our Service Desk. However, because the attacker had sent several e-mails with similar links, one variant did not have sufficient follow-up. We are now investigating how we can prevent this in the future.

2. Technical measures

UM wants to ensure that attackers, if they do 'come in' unexpectedly, cannot get any further inside our infrastructure. To this end, the following actions are necessary:

- Updating the software accurately.

The IT landscape consists of a large amount of software, which has become increasingly complex in recent years. As a result, the number of errors and mistakes in that software has also increased considerably. Suppliers are constantly discovering imperfections in their software and providing updates, which users need to install. To give you an idea: UM receives approximately 100,000 updates per year, all of which have to be processed on 1,647 servers and 7,307 workstations.

These updates are used to close unsafe 'loopholes' in the software. The attackers abused such loopholes at UM. In one case, Fox-IT also failed to determine exactly how the attackers got in.

In another case, it seems that a so-called 'patch' was not installed because something went wrong when the software was updated to a new version.

Further investigation is therefore needed here as well.

- Improving the segmentation of the Windows domain.

Until now, within the Windows domain of UM, the domain administrator account with associated rights was also used for management and maintenance work on regular servers. This is contrary to the existing policy. This made it easier for criminals to gain control of the domain via malware and thus perform malicious actions, such as installing malware and ransomware. In the future, we will therefore monitor the use of domain administrator accounts more closely and restrict their use for maintenance of the domain and the domain controllers. We will also further refine the rights structure within the Windows domain.

UM's network is segmented into so-called V-LANs. These are relatively open to each other to guarantee the openness of the network and also to facilitate decentralised management and

use of UM infrastructures. We now know that a stricter segmentation of the network could have made the movement of malware through the network more difficult. This is a good reason for UM to reconsider the segmentation of the UM network.

- Setting up 24/7 monitoring by means of an SIEM and/or SOC.

The cyber attack has taught UM to better filter signals of abnormal behaviour that end up in the log files. Per second, 30,000 attack attempts are blocked and 1,400 malware attacks per day are stopped. In addition, thousands more signals arrive in various log files every day. We need to make sure that important signals become visible to our administrators faster. To this end, we want to set up a 24/7 SIEM (Security Information and Event Management) as well as a Security Operations Center (SOC), also in consultation with fellow universities. An SOC is a team with the sole task of monitoring cyber threats, advising the institution on security, detecting actual threats and intervening if necessary.

UM was already planning to start such an SOC in January 2020.

As stated in the Fox-IT report, a start was also made immediately on both end-point monitoring and the expansion of network sensors.

- Configuration Management Data Base.

In repairing the damage, a relatively large amount of work was put into clarifying the impact of the attack on the IT infrastructure. There were insufficient insights into the number of active and inactive computer and server systems in the UM domain. In order to gain adequate insights into this, UM wants to map out the 'computer inventory' (Configuration Management Data Base).

3. Double backups

If cyber attackers are unexpectedly able to cause damage, UM wants to be better able to repair the damage itself with backups. Until now, UM has chosen to use backups primarily to provide a working environment as quickly as possible, for example, in the event of a failure or outage. There are several techniques for this. Most commonly used is the creation of so-called 'snapshots' spread over multiple locations. This technique requires that these 'snapshots' are online, depending on the chosen solution or manufacturer.

The cyber attacker was able to encrypt these online backups from a few critical systems. This must be prevented in the future. Therefore, in addition to online backups, offline backups must also be provided, so that the scenario of total failure can be prevented. In the meantime, we have made offline and online backups for every critical system.

Also, users should take into account that—even if there are backups—reinstalling servers always takes extra time and effort. This is unavoidable in order to get the entire configuration up and running again.

Follow-up research regarding data

The Fox-IT report recommends follow-up research into possible 'extraction' of research and personal data. It is true that during the investigation no traces were found in this respect, but UM feels it is its explicit responsibility to have this investigated further. The university will commission Fox-IT to carry out additional forensic research into a number of important data files that are representative of

education, research and business operations. In addition, UM itself will also carry out further research into a number of databases.

Storyline Nick Bos, UM Symposium 5-2-2020

1.

You are visiting Maastricht University today to hear the story behind the cyber attack on our institution.

And that is what we are going to tell you today.

But first I would like to explore a somewhat broader perspective with you, because we are convinced that what happened to us fits into that broader perspective.

"The disruption of society is looming." This alarming message was announced by the **Dutch National Cyber Security Centre** in a news article on 12 June 2019.

A quote: “The digital threat to national security is permanent”.

The Netherlands is vulnerable to digital attacks [...] This is shown in the Cyber Security Assessment Netherlands (CSBN) 2019, prepared by the **National Coordinator for Security and Counterterrorism** and to which the NCSC has contributed.

Three months later, **The Netherlands Scientific Council for Government Policy** published the report Preparing for digital disruption.

A quote, now from the WRR: “In recent years, all kinds of digital disruptions have occurred in the Netherlands and abroad. An important cause for these incidents is cyber attacks. The worrying thing about these incidents is that they also affect vital processes in society. Essential facilities such as healthcare, payment transactions, government services and electricity facilities are at risk as a result.”

These are warnings that seem to have become reality by now. Recently presented national crime figures show that the total number of reports of cyber crime has risen by 64 per cent. Police chief Erik Akerboom reported in the media that he hardly believed his own eyes when he first saw these figures.

In recent weeks, cyber security has been in the news every day—not only because of UM. We have seen reports about banks like Travelex, about a loom factory in Belgium, cities in Germany and Flanders and about hospitals at home and abroad. Ministries, municipalities, the lower house of parliament and other organisations were massively confronted in January with digital vulnerability and with disruption of their daily work due to a security breach in Citrix. On Monday 20 January, this even resulted in 'Citrix traffic jams' on the motorways...

2.

(Higher) educational institutions are no exception to this picture of vulnerability. The umbrella organisations VSNU and The Netherlands Association of Universities of Applied Sciences reported in a letter to the Ministry of Education, Culture and Science in recent days that it is important for everyone to realise that 100% security does not exist: guarantees that cyber incidents cannot be prevented cannot be given by anyone.

We have recently seen examples of problems at the universities in Giessen (Dld) and Antwerp, as well as at Avans University of Applied Sciences, and as a result of the Citrix leak also at fellow universities and at In-Holland University of Applied Sciences where exams had to be postponed.

The annual cyber threat assessment published by the sector shows that cyber threats will only increase more for the sector, with ransomware representing one of the biggest risks. Experts from our own sector and beyond, some of them undoubtedly in the auditorium and tomorrow and Friday at a conference on cyber security in Tilburg, will be able to confirm this.

After all, higher education is vulnerable, as a sector that is constantly looking for the right balance between optimal digital security and providing an open and transparent environment for students and researchers. In their letter to the Ministry, VSNU and VH rightly say that openness is in the nature of educational institutions. Scholars should be able to share information worldwide and participate in different communities. Students do the same and bring their own laptops and tablets. It is extremely complex to take the right security measures without doing too much damage to the nature of our institutions and thus the open character.

VSNU and VH point out that educational institutions themselves bear the ultimate responsibility for good business operations, including integral safety policies. This also includes information security and cyber security. Universities of applied sciences and universities weigh the estimated risks, the impact of the measures to be taken, and the associated costs.

It is important to understand that universities and universities of applied sciences are funded for education and research—and at the time the funding model was created, cyber threats did not yet exist. This means that institutions cannot spend unlimited sums of money on a new function within the institution. Nevertheless, there is ongoing investment in cyber security. This is also necessary because cyber threats also change all the time. There is a real race. Organisations need to respond quickly and effectively in order to remain resilient.

3.

Maastricht University also recognises this permanent threat; the institution has to deal with an average of 1,000 attack attempts per day on its network alone.

These threats are generally successfully dealt with by deploying firewalls and Intrusion Prevention Systems. In addition, it is mandatory to install antivirus software on the workstations and servers and keep it up to date. Thousands of e-mails are also blocked by SURF's SPAM filter (often just advertising, but sometimes there are also phishing attempts).

In addition, the IT Service Desk handles security alerts from around 1000 users a year—people who have received a suspicious e-mail and fortunately report it immediately. These are impressive figures at first glance, but later it will become clear that there is still room for improvement in the area of awareness of digital threats.

4.

On 15 October 2019, there was another such attack. But then things went wrong.

How was that possible?

a. First some general considerations:

- UM is part of a social context in which semi-public institutions have to defend themselves against increasingly professional cybercrime organisations. This defence is an ongoing process, in which UM has certainly not been idle. Extensive AVG measures were taken in 2018 and '19 with a positive effect on the level of the institution's cyber security. In the

autumn of 2019, substantial budget increases were made available for IT in 2020 and beyond, in consultation with the university's management and employee representatives. This included the establishment of a Security Operations Center (SOC). An SOC is a team whose sole task is to monitor cyber threats, advise the institution on security, detect actual threats and intervene if necessary.

- A comparison within the sector—the so-called SURF audit benchmark—shows that from 2017 onwards, UM will show a steady improvement in the extent to which cyber security is effective. For cyber security, the Information Security Higher Education Standards Framework (Normenkader Informatiebeveiliging Hoger Onderwijs, IBHO) has been drawn up on the basis of the ISO27002 standard. This is the most widely accepted international standard for information security and is widely used by Dutch governmental and para-governmental organisations.
- This standards framework forms the basis of the self-assessment system of SURF audit. Whereas currently the medium-term ambition level for most institutions is achieving a score of 3.0 - 3.0+, UM scored 2.58 in 2019 (an increase from a score of 2.08 in 2017). We have no indication that this puts UM below the industry average, rather the contrary.
- UM also takes part in voluntary cyber exercises, which are held by SURF every two years. Institutions jointly practice how to respond to a cyber crisis.
- At the same time, it has to be recognised that, in spite of all the measures and investments, universities are and remain vulnerable in the face of advanced cybercrime organisations.

  What is more, the academic sector and the scientific community—as has already been mentioned—are explicitly asking for accessibility and 'openness', whereas from the point of view of cyber security, ‘closedness’ should be paramount.

  In short, in a world in which cybercrime is becoming increasingly professional and larger-scale, a university must defend itself against this form of crime with limited resources and with an explicit preference for openness and accessibility. It is a race in which you, as an institution, are tested to your limits.
- And universities, like everywhere else, employ people who can be vulnerable to malicious deception both at home and at work. ‘The weakest link is between the keyboard and the chair’, is a well-known saying from the renowned research and consultancy firm Gartner. For the umbrella organisations VSNU and VH, awareness is therefore an important line of action in countering attacks. Awareness is about the awareness of cyber threats and whether, for example, employees and students know that they should not simply click on unknown links in an e-mail.

- In short, systems and procedures can be watertight; people remain an essential link, especially when faced with the challenges of sophisticated and highly professional 'cheaters'.

b. This now brings us to Fox-IT's findings regarding the specific situation at UM.

5.

I am taking you back to 23 December 2019—a moment that will remain forever in the collective memory of our university. UM has been hacked.

Of course, we are prepared for managing crises. We have the protocols; we know our roles and responsibilities; UM has participated in crisis simulations, including cyber attacks.

But the task facing you is huge, in the middle of Christmas time. We immediately formed a Crisis Management Team. One of the first tasks was to call in the right support in this area: Fox-IT was flown in for research and advice. Dozens, and later perhaps as many as two hundred UM employees, did not spend the Christmas holidays undisturbed at home, but worked at least part-time. In addition to the IT staff at central level and in our faculties and service centres, after the first few days many staff members from faculties and support services became involved in addressing the effects of the hack because of their knowledge of educational processes and student welfare .... varying from lecturers and staff of education offices to student advisors, student counsellors, student psychologists, timetable schedulers, help desk staff; policy advisors with legal, financial, HR and academic expertise; staff of the university library, facility services who are involved in the early opening of buildings among other things. And, of course, the employees who took charge of internal and external communication so early on in the process. We were able to call on a great many of our employees and their supervisors. They worked very long days and weeks without a whisper of a complaint and with an enormous loyalty to UM and its students and staff—a sacrifice and endeavour for which we are very grateful.

The administrative tasks were also considerable. Our talent for improvisation was tested; you experience first-hand how dependent you are on systems when you no longer have them. But you have to communicate: with your own community, with the rest of the world. With your stakeholders, internally and externally, from U-Council, deans and directors to the Inspectorate of Education and the Ministry of Education, Culture and Science. And especially your fellow institutions. UM has done everything in its power to warn and inform other universities in good time, in the hope that they will not become victims as well.

Administratively, you are faced with dilemmas every day. What should be done first? How do we organise things? Who and what do we need?

For the EB, it was clear from the outset: the interests of our students, academic staff and support staff are leading. And within that, education comes first. How can we ensure that on 6 January we will be able to have 19,000 students back in the classroom? How can we get 6,000 students to take the exams on the scheduled dates?

6.

However, the biggest question we were faced with was: what to do with the ransom demands of the 'cyber attackers'? We thought about that question very thoroughly. We certainly did not decide anything overnight. We talked about it for a long time. We went over our considerations with deans and directors of UM, the Supervisory Board; we informed the Ministry and the Inspectorate.

And, finally, a well-considered and widely-supported decision was taken on 29 December, about a week after the attack.

In this devil’s bargain, the university had to make an extremely difficult trade-off between two important social interests.

On one side of the scale is the importance of 'not paying criminals'. Although this is not prohibited by law, it is abundantly clear that, for a government-funded institution such as a university, there are some major ethical objections to consider. And as a director, you are horrified by that thought.

On the other side of the scale are the interests of students, researchers, staff and the university. In the sense of (unacceptable) risks concerning academic progress, scientific research, sustainable data security, business processes and ‘in the end’ the continuity of the university.

Weighing these factors ultimately comes down to the degree and duration in which education, research and daily operations are disrupted if the decryption of data and disinfection of systems is not carried out for a long time. Making or having a 'decryptor' yourself is, according to experts, either impossible or will take a very long time (with a duration that is impossible to determine beforehand, if it ever succeeds). And not obtaining a 'key' means that UM must rebuild all infected systems completely from ‘scratch’ and must consider the original, often crucial, data (files) associated with the systems as 'written off' if and insofar as ‘back-up files’ are not available.

In this case, it would take (many) months for UM's education, research and business operations to even be partially up and running again. The damage this would cause to the education and work of students, researchers, staff and the risks to the continuity of the institution would essentially be unforeseeable.

If payment would be made to obtain the ‘decryptor’, the continuity of the organisation could in principle be guaranteed much better and much sooner. It would then be sufficient to clean up existing systems that are infected, a process that would take considerably less time than building new systems and copying saved data from backups.

Faced with this dilemma, the university administration ultimately made an independent decision that was entirely focussed on the interests of students, staff and the institution: acquiring the decryptor.

It is a decision that was not taken lightly by the Executive Board. But it was also a decision that had to be made. We felt, in consultation with our management and our supervisory bodies, that we could not make any other responsible choice when considering the interests of our students and staff. The fact that on 6 January and thereafter we were able to have teaching and exams take place, more or less as planned, that UM researchers suffered little or no irreparable damage, and that we were also able to make the salary payments for 4,500 employees on time, strengthens our confidence that we made the right choice.

7.

UM took and will continue to take responsibility for the choices that have been made and the lessons we have learned.

How?

- by continuing to work on improvements to cyber security that are planned for 2019 and also with the additional recommendations from the Fox-IT report; Michiel Borgers has just told us a few things about this.
- thereby we will also follow a specific and, in our view, crucial recommendation, namely to set up a follow-up investigation into the possible 'extraction' of research and personal data. It is true that Fox-IT did not find any traces of this during the investigation, but we feel it is absolutely our responsibility to have it investigated further.

How?

- by sharing information and findings with as many universities and higher education institutions in the country as possible, either directly or via collaborative bodies such as SURF—a process that was already started on 24/12, less than 24 hours after the attack. Fellow institutions were able to act on it immediately with numerous measures, ranging from increased 'dike monitoring' to actual interventions to neutralise infiltration similar to that at UM.

How?

- by coming out with our story today in the hopes of stimulating a broader discussion and further cooperation. Inspiring examples can be found of successful cooperation in which institutions act collectively. In Canada, for example, a number of universities are working together to create a 'shared security operations centre for higher education'; in the United States this type of joint operations already exists. And, closer to home, healthcare institutions in the Netherlands are working together to set up a security operations centre (SOC), while in Denmark and Switzerland the incident response services of the education sector are working together with other sectors.

8.

It should therefore not be just about UM today.

The cyber attack has been described in the media and in the Lower House of Parliament as a 'wake-up call' for the entire education sector.

The SURF communities SCIPR and SCIRT are already collaborating, especially with UM, and SURFcert was contacted directly during the cyber attack.

But there is still room for improvement. This cyber attack has provided us with important lessons that invite us to work together more broadly, so that we can share not only knowledge but also manpower and investments.

- In concrete terms, discussions have already begun with other educational institutions with aim of establishing a joint service that can provide 24/7 security monitoring, take care of logging, and analyse and share threats among several institutions, or perhaps even for the entire sector.

- this type of 24/7 service could in any case fit in nicely with our local CERT team and with the Security Operations Centre (the so-called SOC), with which UM made a start on 1 January 2020.
- take, for example, mutual cyber security assessments, peer reviews of self-assessments and joint cyber security exercises.

But cooperation alone is not enough. Greater resilience to cyber crime also requires greater investments.

9.

Incidentally, the education sector is not the only sector that is vulnerable. It is good to see that the Ministry of Justice and Security recently, on 24 January, launched a plan in which the National Cyber Security Centre will collaborate more intensively with four sectoral cyber crime teams (healthcare, municipalities, water boards, and education and research – (via SURFcert)).

This brings us to perhaps the biggest lesson we have to learn as a society: do we perhaps have a security issue of the highest order to deal with here? It is not for nothing that journalist-expert Huib Modderkolk has given his latest book on cybercrime and the Internet the title: 'It is war but no one sees it'.

In order to get out ahead of social disruption, shouldn't the thinking and acting on cyber security be taken to a higher level? On a wider scale? In the private and public sectors? In the political domain?

If what has happened to Maastricht University can help bring the debate to that level, at least that's an encouraging thought for us after six very intense weeks!

Management summary Fox-IT report

On 24 December 2019, Maastricht University (hereinafter: Client) contacted Fox-IT B.V. (hereinafter: Fox-IT) regarding a ransomware attack on its infrastructure. This attack had resulted in the encryption of very critical systems for the operational management of the Client. These systems include the e-mail servers, file servers containing research and business operations data, and a number of backup servers. During the incident, Fox-IT provided support in the area of crisis management, and conducted digital forensic investigations.

Fox-IT has determined that the attacker initially gained access to the network of Client by means of two phishing e-mails. These two e-mails were opened on 15 and 16 October 2019 on two workstations, which gave the attacker access to the systems.

From 16 October 2019 up to and including 23 December 2019, the attacker compromised several servers. On 21 November 2019, the attacker, using a server with missing security updates, managed to obtain full rights within the Client's infrastructure. Finally, on 23 December 2019, the attacker deployed the so-called Clop-ransomware on 267 Windows servers. After careful analysis of the possibilities, Fox-IT was informed by the Client on 30 December 2019 that they had decided to pay the ransom.

During the investigation, traces were found that show that the attacker collected data regarding the topology of the network, usernames and passwords of multiple accounts, and other network architecture information. Fox-IT did not find any traces within the scope of the investigation that point to the collection of other types of data. Additional forensic research on critical systems, also referred to as crown jewels, could provide more insights into this.

On the basis of the investigation, Fox-IT has formulated various recommendations that can be classified into the categories of prevention, detection and response:

- Improve processes when it comes to vulnerability and patch management.
- Apply more segmentation within the network architecture and user rights.
- Implement or improve network and log monitoring.
- Practise with different crisis scenarios and improve the plans where necessary.

Finally, Fox-IT recommends critically reviewing the implementation of the above recommendations.