Bernold Nieuwesteeg

Pay to release the hostage?

Will the twenties of the 21st century be as roaring as the twenties of the previous century? Well, from a cyber security perspective, the new decade started in the Netherlands with a blast. Maastricht University experienced a sophisticated ransomware attack that affected almost the entire IT-infrastructure. And a vulnerability in Citrix-software led to a shutdown of systems to work from home by many instances, among them the Dutch House of Representatives (*de Tweede Kamer*). A major debate arose whether it is right to pay ransom.

For me, the reality of the cyber-attack in Maastricht became clearly visible. From my own desk, I could see several colleagues from Maastricht University with a part-time position in Rotterdam pouring into Erasmus University Rotterdam (EUR) in those early days of January. These kind Maastrichtian scholars worked at EUR due to the shutdown of the majority of the IT systems at their home university. In that sense, that partial position at EUR functioned as their own fall-back system because they could still use the EUR IT system.

> "It would give a signal to the world that one could take every Dutch citizen hostage, considering the ransom will be paid after all."

Not that they were entirely safe of course. The EUR itself suffered a data breach in the end of 2016. We know from this experience that Maastricht University will logically intensify its cyber security investments. "When the horse is stolen, the stable-door is locked." Chances are high that there will be a vast increase in the budget of the CIO office, a vast improvement of the cybersecurity systems, security awareness campaigns for staff and students and maybe most importantly, the proper separation of back-up systems (which were also infected). This cybersecurity campaign following the attack will arguably cost several millions.

Naturally, it is important that the right strategies and policies are adopted to lower the likelihood of such an impactful ransomware attack. But we should be aware that the Maastricht University ransomware attack points out the question about the validity to actually pay the ransom. Allegedly, Maastricht University paid a few hundred thousand Euro ransom to the attackers because their back-up systems were infected as well. Hence, for

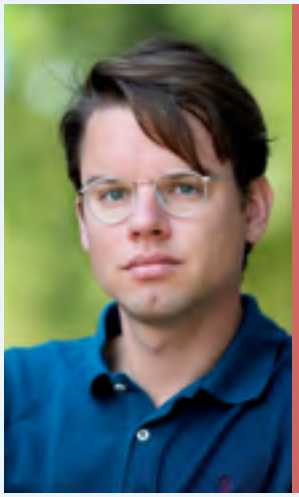
the university, it could have possibly been the choice between paying the ransom or otherwise losing huge amounts of research data, which could contain years of work of thousands of employees and students. Another argument in favour of paying ransom is that most ransomware-attackers are trustworthy. Cybersecurity experts, who frequently deal with ransomware-attacks, can often distinguish 'professional trustworthy cyber-criminals' from unreliable lone wolfs. These professional attackers keep their promises and 'release' the hostage after the ransom is paid and do not attack the victim again.

Hopefully, the criminals who attacked Maastricht University are trustworthy and did not install a backdoor that allows them to take the University hostage again and indeed employees and students can regain access to their data.

But it is also clear that paying ransom reinforces the business model of the cybercriminal. Maastricht University transfers a part of the cost of the cyber-attack to society that arguably can experience more ransomware attacks in the future. That is also the reason why for instance the Dutch Foreign Affairs ministry refuses to pay ransom in the case of an 'offline hostage-taking'. It would give a signal to the world that one could take every Dutch citizen hostage, considering the ransom will be paid after all.

The Dutch police simply do not advice to pay ransom. The FBI published ransomware updated guidelines in fall 2019, stating that it does "not support paying a ransom to the adversary. Paying a ransom does not guarantee the victim will regain access to their data; in fact, some individuals or organizations are never provided with decryption keys after paying a ransom." However, the FBI recognizes that sometimes paying ransomware is the only option when organizations are faced with an extreme loss of continuity, availability and integrity of their data: "While the FBI does not support paying a ransom, it recognizes executives, when faced with inoperability issues, will evaluate all options to protect their share-holders, employees, and customers."

Facing the aftermath of the ransomware attack at Maastricht University and given the fact that companies sometimes pay ransom despite the advice of the police, it is time that also the Dutch government introduces an updated policy advice on how organizations can deal with ransomware attacks most effectively. It would be good if Maastricht University, and other stakeholders from government, academia and industry, are included in the discussion.



About the author
Bernold Nieuwesteeg is director of the Centre for the Law and Economics of Cyber Security at Erasmus University and partner at CrossOver. He regularly advises public and private actors on their cyber security strategy and studies methods to increase knowledge about sensible investments in cyber security.