Comment

Lessons learned from the latest ransomware attacks: Make short work of them.

An assessment by Dominik Lehr, founder and CEO of communication solutions provider Befine Solutions AG

Freiburg im Breisgau, Germany. 8th November 2017. According to Europol, Europe needs to prepare itself for a large increase in the number of cyber-attacks. As it said in its annual report, the threat of internet-based organized crime has reached an "unprecedented scale" and ransomware has put all the other threat types in the shade. The "peak" up to now has been the WannaCry attack in May, in which over 300,000 computers in about 150 countries were infected. Victims included companies in the logistics, telecommunications and healthcare sectors. For example, there were significant disruptions to medical care in Britain, while in Germany display panels and ticket machines in stations stopped working. The vulnerability of our digital infrastructure could hardly be more obvious. It is striking that systems in critical infrastructure are often those that become infected. But here, more than anywhere, it is difficult for the affected companies to respond to the constant demands to update their software. What we need instead is a change of perspective – focusing less on IT and more on the communication processes that dominate in so many companies and public authorities.

Soon after WannaCry, Petya was the next attack that paralyzed companies and public authorities around the world. The victims included banks, utility firms, airports, rail companies, shipping firms, food manufacturers, media organizations and even the Chernobyl nuclear power station. It was caused by a ransomware version that had already been discovered last year and apparently used the same security flaw in older versions of Windows as WannaCry did. At the end of August, the parliament in the German state of Saxony-Anhalt was the victim of a ransomware attack too. Its IT and communication systems had to be shut down and all necessary documents had to be handed out to the members of parliament in paper form.

In these cases, people are all too quick to draw conclusions and make demands. This includes calls to update software and programs immediately. It is true that patching security flaws is generally seen as the first and most effective protection mechanism. The use of security solutions and regular backups should be self-evident anyway even to the most hard pressed IT team. The EU General Data Protection Regulation, which becomes enforceable in May 2018, refers to "appropriate protection" – but what is appropriate?

Taking warnings seriously

Many companies and public authorities are still using operating systems and software programs that have not been supported by the manufacturer for a long time and therefore no longer receive any updates. The patch to plug the WannaCry hole had actually been available for just under two months, but in practice many companies take over 100 days to apply these updates. Although this may seem negligent at first sight, there are often good reasons to delay. Things are not always as easy as they seem on face value.

There are many industries and segments whose computers cannot just be "quickly shut down" and restarted – just like those affected by the attacks mentioned above. Users, whether they are at work or on their home computer, are familiar with the problem too. Updates take time and can be annoying, especially if there are problems once the patches have been installed. It is good practice for IT managers in companies to place a lot of importance on testing patches before installing them.

Rethinking processes

This is why it is necessary to take a different perspective with less of a focus on IT and more focus on the types of communication processes and practices that dominate in so many companies and public authorities. They are part of the problem and make certain areas more vulnerable to attack.

In the Saxony-Anhalt case, for example, a parliament worker activated the malware when he opened an email attachment. He thought he had previously forwarded the mail to himself because his own name was shown as being the sender. The healthcare sector, which has also hit the headlines several times due to ransomware attacks, has its own set of idiosyncrasies such as macros in Office programs that are widely used in hospitals.

But there is some good news. There is just one small area where companies and public authorities need to handle processes differently, enabling them to close loopholes and increase their level of protection ensuring that incoming emails cannot unleash a vicious circle of threats.

Closing loopholes

All it needs is one simple measure that is fast to implement: changing internal workflows and using the appropriate solutions that ensure that predefined file types cannot come in via email in the first place. Instead, companies can receive their emails via their own web application. That way, bots have no chance of spreading malicious code due to the existing authentication measures. With several security levels, the solution makes life more difficult for the attackers, who want to infect as many computers as possible as anonymously as possible.

One last thing, like others, we also recommend not paying ransoms. Firstly, it is questionable whether the victims will be able to access all their data again once they have paid the ransom. And secondly, it just confirms to cyber-criminals that their business model works well and they will receive additional financial support. Instead, anyone affected should involve the police immediately.

About Dominik Lehr
Dominik Lehr is founder and CEO of Befine Solutions AG, an email security company based in Freiburg im Breisgau (Germany) that develops and sells enterprise communication solutions.

About Cryptshare and Befine Solutions
The owner-managed Befine Solutions AG develops and supplies software solutions that help companies support, optimise, and secure their processes. Founded in the year 2000, the company with now over forty employees has its headquarter and development site located in Freiburg im Breisgau, Germany. There are sales locations in the UK and the Netherlands. In 2017, a subsidiary in America was established: Cryptshare Inc.
The focus is on Cryptshare, a communication solution for the exchange of sensitive business information. It makes it possible to send and receive e-mails and large files ad-hoc – secure, easy and at low cost. Cryptshare also offers auditability which helps companies to follow compliance rules and regulations. Today more than 1000 companies in over 30 countries use Cryptshare with about 2.5 million users. This success is underlined by the "Cybersecurity Excellence Award 2017". Please find further information on: www.cryptshare.com. Users may inform themselves on the blog.

Press contact:
phronesis PR GmbH
Marcus Ehrenwirth, Marcus Wenning
Kobelweg 12 ¼
D-86156 Augsburg
Telephone: +49 821 444800
Email: info@phronesis.de
Web: www.phronesis.de

Befine Solutions AG – The Cryptshare Company
Oliver Gäng – Head of Digital Marketing
Schwarzwaldstraße 151
79102 Freiburg im Breisgau
Germany
Telephone: +49 761 389130
Email: oliver.gaeng@cryptshare.com
Web: www.cryptshare.com