HealthManagement
Promoting Management and Leadership

Volume 16 - Issue 3, 2016 - In the News

No More Ransom

Mag. Christian Marolt
Executive & Editoiral Director
HealthManagement.org
******@***marolt.com
LinkedIn Twitter Facebook

There are two simple yet effective preventive measures that a public or private enterprise must put into place to stop cybercriminals in their tracks says Europol; practice pristine digital hygiene and keep anti-virus protection up-to-date.

While these steps should be taken as the bare minimum to protect an organisation, if the dramatic increase in cybercrimes is anything to go by, they are being widely overlooked. According to Kaspersky Lab, the number of users attacked by crypto-ransomware rose by 5.5 times, from 131 000 in 2014-2015 to 718 000 in 2015-2016. Ransomware is a top threat for EU law enforcement: almost two-thirds of EU Member States are conducting investigations into this form of malware attack.

Ransomware attacks on healthcare facilities are increasing with reports of incidents hitting the headlines on a regular basis. “The increase has been evident over the past three to five years,” a Europol spokesperson told HealthManagement. org. “There are two things you can do immediately to protect your organisation from cyberhacking. Firstly, exercise digital hygiene amongst staff. This means staff need to be educated to not open emails from unknown sources for example. The second is to keep your anti-virus up to date. It’s amazing how organisations fail to implement these two basic measures and how much disruption this can cause.”

With staff so central to the prevention of potentially devastating cyberattacks, it may come as a relief to healthcare facilities that Europol said, contrary to some media reports, the law enforcement body is not aware of widespread cases of personnel actually cooperating with cybercriminals.

HealthManagement.org was speaking to Europol after its July launch of No More Ransom, a website initiative by Europol’s European Cybercrime Centre, the National High Tech Crime Unit of the Netherlands’ police and two cyber security companies – Kaspersky Lab and Intel Security. The goal is to help victims of ransomware retrieve their encrypted data without having to pay the criminals. The initiative is open to other public and private parties.

The site provides a guide to what ransomware is, how it works and, most importantly, how to ensure protection of data. The project provides users with tools that may help them recover their data once it has been locked by criminals. In its initial stage, the portal has four decryption tools for different types of malware, the latest developed in June 2016.

“Cybercrime has changed a lot in the last few years. Hackers are becoming more professional and aggressive.” If a hospital or other healthcare facility is successfully hacked Europol said that management of the body should not hesitate to report the incident to police.

“It is critical that when an organisation is hacked, that they report it to police right away,” the spokesperson said. “We have fortunately noticed a trend toward this while before, the instinct of many companies was to keep it under wraps because they didn’t want a negative impact on their reputation. But the role any hacked enterprise plays in fighting cybercrime is very important and the first step is reporting as soon as they detect a data breach. Europol can support a hacked organisation and help them retrieve their data.” Under no circumstances should an organisation pay the cybercriminals, No More Ransom says.

“Paying the ransom is never recommended, mainly because it does not guarantee a solution to the problem. There are also a number of issues that can go wrong accidentally. For example, there could be bugs in the malware that makes the encrypted data unrecoverable even with the right key.”

In addition, if the ransom is paid, it proves to the cybercriminals that ransomware is effective. As a result, cybercriminals will continue their activity and look for new ways to exploit systems that result in more infections and more money on their accounts, the initiative says. While No More Ransomware describes itself as ‘outreach’ for the public, most details of Europol’s cybercriminal-fighting activity is kept firmly under wraps for security reasons.

“I’d like to think that we will get ahead of cybercriminals – our team is made up of the best in Europe,” said the spokesperson. “We’re bringing hackers to justice every day but this information is not publicly releasable as arrests and investigations across pan-European cybercriminals networks continue. Eventually we will bring down cybercriminals.”

For details on No More Ransom go to: nomoreransom.org Europol produces an annual Internet Organised Crime Threat Assessment (IO CTA) document with information on the state of cybercrime in Europe, key findings, operational priorities and general observations. The next document will be available online at the end of September at: europol.europa.eu/iocta

Published on : Thu, 25 Aug 2016