South China Morning Post 南華早報

WannaCry ransomware attack shows the wisdom of having an offline Plan B

PUBLISHED : Thursday, 18 May, 2017, 11:24am
UPDATED : Thursday, 18 May, 2017, 11:24am
Comment › Insight & Opinion

Kai-Lung Hui

Kai-Lung Hui says organisations providing critical services must have a backup plan that does not rely on the internet in case of a crippling cyberattack

The latest [1] [1] ransomware attack [1] sent the world into turmoil this week. Malicious software called WannaCry infected more than 200,000 computers worldwide, locking out users unless they paid a ransom in bitcoins to the attackers. Some of these locked computers are used in hospitals, petrol stations, schools and power companies.

Most IT security specialists advise victims not to pay such ransoms, but some organisations may feel they have no choice. After all, peoples' lives could be in danger if, say, medical practitioners cannot access health records.

'Ransomware' attack shows the time has come for a digital Geneva Convention [2]

This raises a pressing issue: when technology is so embedded in our daily routines and incorporated in rudimentary services such as health care and the provision of utilities, how can we reduce our risks in the event of a cyberattack?

In the case of WannaCry, IT experts have advised us to patch our operating systems, use anti-virus software and firewalls, and not to download files or open email attachments from unknown sources. This is good and practical advice, but it is insufficient at a time when cyberattacks are evolving fast and new means of attack are constantly emerging.

The next ransomware attack will likely be worse than WannaCry [3]

Today, novice hackers do not even need to know how to write encryption programs; they can deploy off-the-shelf ransomware to blackmail others. Some underground criminals offer dial-a-hacker services on the "dark web", the encrypted segment of the internet not familiar to most users.

No doubt, defence tactics such as enabling firewalls or performing frequent backups will not suffice in the near future.

Worst of WannaCry may be over but the 'cyberattack game has changed' [4]

What we need is a change in attitude. Instead of betting everything on protection and defence, we should prepare for a scenario when the operating system is unavailable or critical data is not accessible from a computer. Hospitals should still be able to prescribe medication and conduct surgery when patients' health records cannot be retrieved from servers. Power companies should have a backup system that can immediately take over the job and maintain the electricity supply to critical infrastructure services, in case of a security breach.

Preparing for such alternative systems is inevitably costly. But when IT is used as an integral part of services that affect people's lives, we need to ensure that these services can continue when the system fails. The WannaCry attack shows this may not be the case with many organisations. It is now time for organisations, especially those providing critical services, to evaluate their contingency plans for when their IT systems fail; a "Plan B" is necessary, and this had better be one that can function without the internet.

Kai-Lung Hui is a professor at the HKUST Business School. The views expressed here are his own

Topics: Cybersecurity

More on this:
Hong Kong firms urged to sharpen focus on cybersecurity [5]
Is your PC up to date? Home computers exposed as global cyberattack threat builds [6]

Links
[1] http://www.scmp.com/tech/enterprises/article/2094463/ransomware-cyber-assault-slows-focus-turns-catching-hackers-who
[2] http://www.scmp.com/comment/insight-opinion/article/2094454/ransomware-attack-shows-time-has-come-digital-geneva
[3] http://www.scmp.com/lifestyle/article/2094628/next-ransomware-attack-will-likely-be-worse-wannacry-warns-security-tech
[4] http://www.scmp.com/news/china/policies-politics/article/2094576/worst-wannacry-may-be-over-cyberattack-game-has-changed
[5] http://www.scmp.com/tech/enterprises/article/2089632/hong-kong-firms-urged-sharpen-focus-cybersecurity
[6] http://www.scmp.com/news/hong-kong/law-crime/article/2094299/hong-kong-smes-home-computer-users-especially-risk-global