Volume 16 - Issue 1, 2016 - Spotlight

Big Drama in IT Security

Recent Hospital Virus Attacks Trigger Call to Redefine IT Security

Recent cases of cyber-attacks, intentionally breaching the security infrastructures of hospitals around the globe, have raised serious questions about how to tackle such malicious invasions. no matter if it was for financial gain or the simple thrill of having broken through the iron-clad firewalls set up by it giants.

The European association of healthcare it Managers (HITM hitm.org) has no time for the FBI’s stance on how hospitals should deal with hacker attacks.

While last autumn the U.S. intelligence agency controversially advised organisations to give in to criminals who paralyse their IT systems and pay the ransom to regain access to information, the HITM says the problem needs to be dealt with at a deeper level.

“We encourage software vendors to invest more in security, and our members and the it community in general to set up systems that are not vulnerable to hacking,” HITM secretary General, Christian Marolt told HealthManagement.org.

“A government will never pay ransom for the release of a citizen held hostage, as it will just trigger more such incidents; we firmly believe that healthcare shouldn’t give in to hacking blackmailers either.”

The HITM endorses the professional authority and responsibility of healthcare it managers and represents their interests to international institutions and associations.

Marolt was speaking following the infamous payment of what was reported as 40 Bitcoins or 17,000 U.S. dollars to unknown blackmailers by the Hollywood Presbyterian Medical Center after its it systems were brought to a standstill by ransomware in early February.

Reportedly, staff were forced to return to the not-so-distant ‘old days’ of communication by phone and fax, while emergency patients had to be transferred to neighbouring hospitals. But the high-tech hospital said that patient records were never compromised during the attack by the ransomware virus.

Security Focus

“We urge any hospital to reject a ransom request,” Marolt said. “The emphasis must be put on better security. There are still hospitals in Europe operating on last-century legacy, not able to deal with these kinds of attacks.”

Marolt added that we seriously need to question our it security when a simple malicious email, opened in error, can bring any size hospital to a standstill. Consider the outcry if this would happen to an airliner!

“When you reflect on the pressure and level of stress hospital staff is exposed to, how can you be surprised that one may open a malicious email by mistake?”

Ransomware is a type of malware that locks a computer’s functions until a fee is paid by the owner of the computer or network. Typically, computers display a message with a countdown timer that threatens the wiping of all data stored on the computer if the ransom is not paid on time.

The preferred hacker currency is Bitcoin, a digital currency created and held electronically. It is not under the control of any sole person or body and neither is it printed. Why do hackers use it? It is nearly impossible to track once it is released.

The FBI and other organisations like the German Bundesamt für Sicherheit in der informationstechnik (BSI) warned about the vulnerability of the healthcare sector in 2014 and the following year saw a sharp rise in cyber-attacks. Under U.S. government law, hospitals are obliged to report potential breaches of medical data security, if they involve more than 500 people. In Europe, the laws are not so clear.

A cyber-attack brought the almost fully paperless Lukas hospital in Neuss, north Rhine-Westphalia, Germany to a standstill for two weeks. This raised serious concerns about the lack of pan-European reporting protocols when dealing with such malicious viruses.

The IT systems of the 540-bed hospital were infected by a virus, which experts said had been sent as an email attachment and probably opened by mistake. As with Hollywood Presbyterian, severe emergency department (ED) cases were transferred to other hospitals.

After the attack, the hospital confirmed in a statement that the cause for the breakdown was a malicious virus sent from an unknown source, but added that the action did not appear to be targeted, as there was no blackmail attempt. Top IT experts from Germany and the UK had to be called in to get the problem under control.

Source: rp-online.de

Hidden Attacks

However, the HITM praised the Lukas hospital for being transparent about the attack. “A serious worry seems to be the lack of clear criteria in IT security law for reporting on cyber-attacks. Lukas Hospital made a courageous step forward to immediately inform the public. This transparency encourages trust in the institution and helps to counter future attacks much more easily,” said Marolt.

According to German media, two other hospitals and a company had also been affected by the virus around the same time, but the incidents had not been made public. “In such context serious questions have to be asked:

- How many companies in Europe, and around the Globe, apply ‘strict secrecy’ over cyber-attacks and cover them up?

- How many of them pay ransom?

- and how many hide financial losses from such attacks cleverly in their balance sheet?” Marolt asked.

The cyber-attacks lead to bigger questions about the impact of technology in healthcare. You only have to consult one of the many bespoke groups representing patient interests to discover that the takeover of healthcare by IT is not all coming up smelling of roses.

While IT applications like the employment of Big Data in diagnostics and Geographic Information Systems for improving workplace management and upgrading patient care are paving the way for better outcomes, there are still many people who aren’t yet convinced about the benefit in using an app over a face-to-face consultation.

That’s not to home in on mHealth either which, as with all new and developing technology, has pros and cons. across the board, from the use of Electronic Health Records to robotically-assisted surgery, while one hand gives with cutting edge technology, the other takes away with the amount of time, training upgrades and expense needed to implement the full panoply of IT applications at medics’ disposal.

While governments and NGOs tout paperless hospitals, spending billions on the process of reaching this goal with the aim always to ‘improve care’, at what cost - both literally and ethically? Take the National Health Service in England, for example, which just announced a 4.2 billion pound investment plan for bringing care into the modern age by 2020. When digitalisation does not go hand-in-hand with a dramatic upgrade to state-of-the-art IT infrastructure, we are playing digital “Russian roulette”.

What will happen if hospitals do give in to the ransom demands of cyber- blackmailers? The ‘reassuring’ comments about the safety of patient data, and that ransom fees are not that high after all, just don’t add up. What does it really mean for the IT security future of hospitals?

“Today hackers may demand a few thousand dollars and lock a computer system for a few days,” said Marolt. “But if they’re successful, what about tomorrow?”

Key Points

- Cyber-attacks are on the rise, and hospitals have fallen victim.
- Controversially, the FBI advised organisations to pay ransoms to regain access to their information.
- The European Association of Healthcare IT Managers recommends tightened security, and transparency from hospitals that are attacked.

Published on : Sat, 27 Feb 2016