nccgroup

Shutterstock: Royalty-free stock photo ID: 574043182

Jun 26, 2020 21:52 BST

Hospitals and ransomware: The human cost of weak cybersecurity

By Sourya Biswas, Principal Security Consultant, NCC Group

While data breaches have been the most prominent consequence of cyber attacks in the last decade, ransomware attacks have been fast catching up. And if you've been following the news around ransomware, you will have noticed just how often hospitals are featured as the victims. As events in

the US, France, and Romania show, ransomware in healthcare is a global problem.

Why all the attention on ransomware? It has to do with the nature of the attack. To put it simply, ransomware a class of malware that prevents users from accessing their system or personal files and demands ransom payment in order to regain access. Therefore, while data breaches affect the confidentiality of data, ransomware affects its availability. The development of cryptocurrency, which facilitates anonymization of payments, has contributed to the recent increase in ransomware attacks. By offering a payment mechanism that is easy to verify, but difficult to trace, cryptocurrency has made ransomware quite lucrative for bad actors.

Coming back to healthcare, I believe there are three primary reasons why hospitals are disproportionately targeted in ransomware attacks: inherent insecurity, high cost of medical systems, hospitals' propensity to pay.

1. Inherent insecurity of medical systems

It's not unusual for a medical system manufacturer to include verbiage in the contract that the warranty would be broken if the user organization were to modify the device in any way. Even if such equipment uses a deprecated operating system like Windows XP, the hospital is unlikely to attempt to secure it at the risk of voiding the warranty. Not to mention that many medical systems are regulated by the US FDA (Food and Drug Administration) that make it virtually impossible for hospitals to update them themselves.

2. High cost of medical systems

Unlike the typical industry using standardized equipment, hospital equipment is often highly specialized and costs significantly more. Consequently, they are difficult to replace, especially on short notice. While you can easily go out and buy a server off the shelf, or may even have one in storage, the same is unlikely to be true for a Magnetic Resonance Imaging (MRI) machine.

3. Hospitals' propensity to pay

The third reason is linked to the first. Since hospital equipment is hard to replace, there's an incentive to pay the ransom justifying the cost as less than the cost of replacement. This line of reasoning becomes even more pressing when one considers what's at risk – human lives. Whereas a bank hit by ransomware may not be able to process transactions and cost its customers money, a hospital unable to run its systems will impact its ability to treat patients and may even result in deaths. When weighed against human lives, material wealth becomes immaterial. There may be a less altruistic and more cynical reason at play here as well. HIPAA fines are quite high, and while there may be an argument if locked-but-undisclosed

information falls under its scope, the temptation to just "pay and make the problem go away" without performing a formal breach risk assessment and possibly informing federal authorities.

Guidance for healthcare organizations dealing with ransomware

This is a very dangerous world we live in and we can't expect cyber-attackers to treat hospitals any differently than how they view other targets. In addition to detailed assessments to identify security gaps and address them, here are some high level recommendations that hospitals should look to implement:

Backup patient data

Patient data should be regularly backed up. There should be very restrictive connectivity between the hospital and backup environments to prevent ransomware spreading and infecting the latter. A robust process should be developed to backup and secure patient data. Backup processes and technology should have additional scrutiny placed on them as they are the last line of defense for maintaining business processes.

Change default passwords

In my experience, many hospitals don't change the default passwords on their equipment, persisting with whatever was configured by the manufacturer during setup. That leaves them open to attack by anyone who knows the default password, either through a leak at the manufacturer or by another hospital that has already been compromised. Moreover, changing the password to "password" or "1234" doesn't count; strong passwords should be implemented. Alternative solutions, like biometrics or proximity cards (considering current COVID-19 concerns that make biometrics a concern), while more expensive to implement, are easier to use in some circumstances and will get less pushback from users.

Implement the principle of Least Privilege

Another gap that I have noticed is that everyone on the hospital floor has access to all kinds of medical equipment. Ideally, only those people who need access to specific equipment to do their jobs should have access to said equipment. This is true for physical access and logical access as well (see point 2 above). However, this should be implemented such that patient safety is not compromised. We don't want a situation where the only person who has access to certain lifesaving equipment is not available in a life-or-death situation.

Disable unnecessary connectivity

While many pieces of equipment have the ability to connect to networks, that doesn't mean they have to. Connectivity to networks should be based completely on what's needed and any unnecessary connectivity should be

disabled.

Secure hospital networks

The hospital network should be segmented from the public Internet using a firewall (ideally more than one from different manufacturers). Firewalls should be configured to allow only approved traffic to go through, both from outside and inside. Building on this approach, it may make sense to implement micro-segmentation and gradually move to a zero-trust model. Depending on sensitivity of data, internal traffic should be encrypted.

Provide security awareness training

People are considered the weakest link in cybersecurity and even with the best of tools, attackers succeed because victims let them in. Train hospital employees to observe good security practices like strong passwords and not to respond to common social engineering attacks like phishing. Hospitals should realize that cybersecurity training is not a cost, but an investment to prevent significantly higher future costs. Consequently, such training should be identified as a mechanism to meet business needs like operational resiliency, regulatory compliance and reputation management. Also, if cyber insurance is to be effectively leveraged, employee training will be part of the hospital's "due care" requirements.

Perform continual security improvements

Establish methods to ensure the security of medical devices (patching, configuration, etc.), through contract or agreement on internal hospital support. Maintain a process to identify and address vulnerabilities via scanning and penetration testing. The success of such a vulnerability management program is predicated on accurate inventory (asset management) and change control (configuration and change management).

About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 15,000 clients worldwide to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience and global footprint, it is best placed to help businesses identify, assess, mitigate and respond to the evolving cyber risks they face.

To support its mission, NCC Group continually invests in research and innovation, and is passionate about developing the next generation of cyber

scientists.

With over 1,800 colleagues in 12 countries, NCC Group has a significant market presence in North America, continental Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia and Singapore.

Contacts

Regional Press Office - North America
Press Contact
NCCGroup@cdc.agency
+1 408 776 1400
+1 408 893 8750