HealthManagement
Promoting Management and Leadership

Volume 16 - Issue 2, 2016 - In the News

Prognosis Negative

James Scott
******@***icitech.org

Senior Fellow at the Institute for
Critical Infrastructure Technology
(ICIT) Washington, U.S.

THE HEALTH SECTOR’S CYBER -HYGIENE EPIDEMIC

Nietzsche said, “*All great things must first wear terrifying and monstrous masks in order to inscribe themselves on the hearts of humanity* ”. Unfortunately, for the health sector the issues of ransomware, malware and hackers must worsen before things improve. This is not a sadistic estimation; rather, it is a prediction that the healthcare communities victimised by cybersecurity attacks will not be galvanised to action until significant impact has already occurred. Sadly, only after the threat is tangible, and the attack surface left unobscured will organisations shift their culture to address the threats looming on their threshold.

The latest digital epidemic to take the healthcare sector by storm is crypto ransomware. Ransomware is nothing more than weaponised encryption. It is unique in cybercrime because in order for it to be successful, it requires the victim to become a willing accomplice after the fact. Ransomware is dangerous because it requires virtually zero technical aptitude, so practically anyone can do it. Healthcare organisations, which used to be off-limits to cyberadversaries, are now the primary targets of many cyberthreats. This shift occurred recently, when healthcare organisations began digitally retaining more customer data, and when hospitals such as Hollywood Presbyterian hospital began to pay to end ransomware and other attacks.

The Threat: Facts

There are two primary cyber-criminal groups that capitalise on these unique attack vectors against hospitals; script kiddies and hackers for hire (aka Mercenary Hackers). Script kiddies are the toxic, parasitic ‘hacker wannabes’ clinging to the fringes of dark web forums. They possess limited, if any, tech sophistication and wreak havoc on the global population by spamming ransomware without any particular target. They are able to capitalise off of the few people that fall for the spoofed emails that read as if they are coming from online retailers or payment systems, for example. On the other hand, Mercenary Hacker Teams are usually technologically sophisticated and precise in their selection of victims. They write their own multi-tiered code, and they have more structured agendas behind their attacks. They may use ransomware as a diversionary tactic to create organisational chaos at the premises of their target while simultaneously penetrating the network from another angle in order to exfiltrate sensitive data, only to manipulate remaining data when their mission is accomplished. Whether the ransom is paid or not paid is not their true motivation; instead the exfiltration, manipulation, or destruction of valuable sensitive data is their primary aim. They repeatedly and systematically monetise stolen information over and over again on multiple dark web forums to endless clients who stem from an infinite variation of motivations.

Sophisticated hackers will target organisations deficient of at least a general baseline: the lack of cyber hygiene, the prevalence of bureaucratic siloes that host unique interorganisational political feuds, the dependence on an IT team instead of a qualified info-sec team for cybersecurity, and most importantly, hackers will target organisations where employees are under-appreciated, over-worked and underpaid. Organisations with these characteristics will be targeted and in most cases, adversaries will succeed in the attack.

In short, the adversaries are numerous, the attack vectors are hyper-evolving, and the stealth and sophistication of even upstarts in the hacker sphere are becoming even more creative and devastating. In this type of environment, fear mongers are omnipresent and will attempt to offer silver bullet solutions to fearful organisations. Make no mistake; there is no silver bullet solution to the vast hacker and script kiddie conundrum. Instead, a layered defence is the only meaningful method of defence. A persistent attacker will breach any defensive perimeter. It is important to realise that you cannot keep a breach from happening; you can only detect and respond to threats. The good news is, many technologies exist that can severely minimise your organisation’s attack surface in order to thwart threat.

Dealing With the Threat

First, give your IT team a break. Chances are, they are not qualified to maintain your organisation's cybersecurity posture and it’s time to bring in a cybersecurity team whose sole purpose is information security. Organisations that are too small or lack the financial resources to hire a dedicated team, need to lease a team or license the services of a credible vendor.

The first thing the infosec team will do is run a risk assessment on your organisation and patch vulnerabilities immediately. They will educate staff on the latest threats and how to mitigate vulnerable systems. Then they will create policies and procedures that are security-centric, they will audit third parties who have access to your network for cyber hygiene, and they will report their findings and progress to the board quarterly.

From a technical perspective, they will introduce a layered cyberdefence that will evolve with emerging threats within the industry. They will implement layers such as endpoint security, ongoing patching, continuous penetration testing, user behaviour analytics and other user/network abnormality detection mechanisms, encryption of data that is in transit and stationary, threat intelligence and least privileged user credential policy among staff and most importantly, they will begin backing up data in real time. The information security team will do everything that they were trained to do to prevent intrusions in the network and to remove threats before incidents occur.

The Time to Act is Now

Organisations must evolve with the threat and make use of technologies that already exist in order to combat the legions of invisible adversaries who are continuously analysing and testing their networks for exploitable vulnerabilities. Adoption of an information security team is how organisations evolve. The healthcare sector is known for its glacial pace of reform. In the next year or two, organisations which fail to adopt an information security team will become notorious in the community as the organisations that succumbed to an incident.

For long-term defence across the healthcare sector there must be a renaissance in cybersecurity that promotes cyberhygiene and a security-centric organisational culture that is continuously reinforced by peer pressure. If the community expectation rises to include information security as a requirement, then additional regulation will not be needed and attackers will divert to easier targets in other sectors. If organisations fail to adapt to the looming threat, then more predatory adversaries will flock to the vulnerable prey and the only way to halt the barrage of attacks will be drastic regulation-based reform.

Key Points

- Healthcare is now a key target of cybercriminals.
- Generally, there are two types of hackers; unsophisticated Script Kiddies and tech-savvy Mercenary Hacker Teams.
- Securing a ransom is not the main aim of hackers; extracting data for repeated monetisation is.
- Cybersecurity is too stressful for the average IT team. Healthcare facilities need to engage information security experts to protect against cyber attacks.
- Failing to adopt the right professionals will seriously compromise an organisation’s reputation.
- Without adoption of proper security, severe regulation-based reform may be the only option.

Published on : Fri, 1 Jul 2016