HOME CYBER DEFENSE

ARE YOU SAFE FROM CYBER CRIME?

WEEKLY

Volume #4 - Issue #159
May 11th, 2018

This is a weekly publication dedicated to your personal cyber security. Our newsletter is designed to help the public recognize and avoid cyber threats while they are online. If you are not a subscriber, please go to HomeCyberDefense.net to sign up.

Why Hackers Love Healthcare

The number of ransomware and other malware attacks is rising incredibly fast in the healthcare industry, putting human lives as well as critical data at risk. From 2011 through 2014, the sector — including hospitals, labs, pharmacies, drug companies and outpatient clinics — experienced the highest number of data breaches of all industries. What makes these organizations such a popular target?

1. Highly Valuable Data: Commonly, a single stolen credit card number yields an average $2,000 profit and quickly becomes worthless. Healthcare data, however, such as PHI or PII, is extremely valuable on the black market. A single PHI file, for example, can yield a profit of up to $20,000. This is mainly because it can take weeks or months for a healthcare data breach to be discovered, enabling cybercriminals to extract much more valuable data. Moreover, because healthcare data can contain dates of birth and Social Security numbers, it is much more difficult or even impossible to change, so thieves can take advantage of it for a longer period of time.

2. Lack of IT Investment and Training: Most healthcare organizations spend just 3% of their IT budgets on security, while the SANS Institute — the largest provider of cybersecurity training and certifications — recommends spending at least 10%. For most healthcare organizations, security is often an afterthought. They don't provide regular cybersecurity training for their employees, which could help reduce insider threats. For example, 18% of healthcare employees say they're willing to sell their login credentials for between $500 and $1,000. And about one-quarter of healthcare employees know someone in their organization who has engaged in this practice.

3. Highly Connected Systems: Having shifted workloads to the cloud, healthcare organizations have highly connected systems that run the risk of being deeply affected even if the attack takes place on smaller, partial systems. In other words, a cyberattack in one place could bring down the entire system. In May 2017, the WannaCry ransomware attack forced multiple hospitals across the United Kingdom to turn away ambulances transporting patients and cancel surgeries that were within minutes of starting. Even basic processes like admitting patients and printing wrist bands were compromised.

What can the healthcare industry do to mitigate cyber threats? To begin with, the industry must realize that cybersecurity is human-centric. Gaining insight into the normal rhythm of users' behavior, for example, or the flow of

data in and out of the organization improves risk response. Additionally, the industry should be aware that cybersecurity isn't just the responsibility of the IT department: everyone should be aware of the risks, from management down to brand-new contract staff. Healthcare security professionals need to understand the threats they face and the regulations they must comply with, and they must be provided with best practices for strengthening cybersecurity defenses. This means implementing comprehensive security awareness training that educates all personnel on current threats, red flags to look for in an email message or web link, how to avoid infection, and what to do in case of an active exploit. And since the threat landscape is constantly changing, training should be repeated and updated on a regular basis. Additionally, implementing the right cybersecurity measures, such data loss prevention, user behavior analytics, and endpoint security technologies, will further protect an organization's infrastructure and patient data from ransomware attacks. By creating a system that guards the human point — where people interact with critical business data and intellectual property — and takes into account the intersection of users, data, and networks, the healthcare industry can improve its cyber threat protection.

Thank you for subscribing to our email!