HHS Office for Civil Rights in Action

Spring 2019 OCR Cybersecurity Newsletter
April 3, 2019

Advanced Persistent Threats and Zero Day Vulnerabilities

An advanced persistent threat (APT) is a long-term cybersecurity attack that continuously attempts to find and exploit vulnerabilities in a target's information systems to steal information or disrupt the target's operations.[1] Although individual APT attacks need not be technologically sophisticated, the persistent nature of the attack, as well as the attacker's ability to change tactics to avoid detection, make APTs a formidable threat.

APTs are a serious threat to any information technology (IT) system, but especially those that are part of the health care field. Healthcare services are part of a multibillion dollar industry that utilizes data to develop new drugs and treatments. Medical research information, experimental treatment testing results, and even genetic data are valuable targets for theft because of their value in driving innovation. Further, health information is used by healthcare providers and insurers to provide and pay for healthcare services for individuals. If compromised, health information can be used for identify theft that could lead to financial fraud including theft of health insurance coverage benefits. Also, because an individual's health information can contain details concerning the most private and personal aspects of one's life, the compromise of one's health information could also lead to an ability to blackmail an individual based on their sensitive health information. Any security incident impacting the confidentiality, integrity, or availability of protected health information (PHI), can directly affect the health and safety of citizens. APTs have already been implicated in several cyberattacks on the healthcare sector in the U.S. and around the world.

Zero Day Exploits

One of the most dangerous tools in a hacker's arsenal is the "zero day" exploit or attack which takes advantage of a previously unknown hardware, firmware, or software vulnerability. Hackers may discover zero day exploits by their own research or probing or may take advantage of the lag between when an exploit is discovered and when a relevant patch or anti-virus update is made available to the public.

These exploits are especially dangerous because their novel nature makes them more difficult to detect and contain than standard hacking attacks. The possibility of such an attack emphasizes the importance of an organization's overall security management process which includes monitoring of anti-virus or cybersecurity software for detection of suspicious files or activity. Though hackers may exploit zero day vulnerabilities to gain unauthorized access to an organization's computer system, appropriate safeguards, including encryption and access controls, may mitigate or even prevent unauthorized access to, or loss of, protected information. Once zero day vulnerabilities are made

public, this information becomes accessible to both good and bad actors alike which means entities should have measures in place to be aware of new patches and for assessing the need to apply them. In the event a timely patch is not available, or cannot be immediately implemented (such as when testing is needed to ensure that the patch works with components of an entity's information systems), an entity may consider adopting other protective measures such as additional access controls or network access limitations to mitigate the impact of the zero day vulnerability until a patch is available.

A Dangerous Combination

APTs and zero day threats are dangerous enough by themselves. An APT using a zero day exploit can threaten computers and data all over the world. One such example is the EternalBlue exploit. EternalBlue targeted vulnerabilities in several of Microsoft's Windows operating systems. Soon after the EternalBlue exploit became publically known, the WannaCry ransomware was released and began spreading, eventually infecting hundreds of thousands of computers around the world. The damages due to WannaCry infections are estimated to be in the billions of dollars. Analysis of WannaCry found that it used EternalBlue to spread and infect other systems. One of the organizations most impacted was the United Kingdom's National Health Service (NHS) which had up to 70,000 devices infected, forcing healthcare providers to turn away patients and shut down certain services. Several HIPAA covered entities and business associates in the United States were also affected by this cyberattack.

What Can HIPAA Covered Entities and Business Associates Do?

There are many security measures that organizations can proactively implement to help mitigate or prevent the damage that an APT or zero day attack may cause. The HIPAA Security Rule requires security measures that can be helpful in preventing, detecting and responding to cyberattacks such as those perpetrated by APTs or hackers leveraging zero day exploits. The HIPAA Security Rule includes the following security measures that can reduce the impact of an APT or zero day attack:

- Conducting risk analyses to identify risks and vulnerabilities (See 45 CFR § 164.308(a)(1)(ii)(A));
- Implementing a risk management process to mitigate identified risks and vulnerabilities (See 45 CFR § 164.308(a)(1)(ii)(B));
- Regularly reviewing audit and system activity logs to identify abnormal or suspicious activity (See 45 CFR § 164.308(a)(1)(ii)(D));
- Implementing procedures to identify and respond to security incidents (See 45 CFR § 164.308(a)(6));
- Establishing and periodically testing contingency plans including data backup and disaster recovery plans to ensure data is backed up and recoverable (See 45 CFR § 164.308(a)(7));
- Implementing access controls to limit access to ePHI (See 45 CFR § 164.312(a));
- Encrypting ePHI, as appropriate, for data-at-rest and data-in-motion (See 45 CFR §§ 164.312(a)(2)(iv), (e)(2)(ii)); and
- Implementing a security awareness and training program, including periodic security reminders and education and awareness of implemented procedures concerning malicious software protection, for all workforce members (See 45 CFR § 164.308(a)(5)).

Additional Resources:

- Guidance on Software Vulnerabilities and Patching
  https://www.hhs.gov/sites/default/files/june-2018-newsletter-software-patches.pdf - PDF

- HHS Update: International Cyber Threat to Healthcare Organization
  https://files.asprtracie.hhs.gov/documents/hhs-update-4-international-cyber-threat-to-healthcare-orgs.pdf - PDF

- An Efficient Approach to Assessing the Risk of Zero-Day Vulnerabilities
  https://www.nist.gov/publications/efficient-approach-assessing-risk-zero-day-vulnerabilities

- Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems
  https://csrc.nist.gov/publications/detail/sp/800-160/vol-1/final

* *In general, OCR's newsletters do not establish legally enforceable responsibilities. Instead, these newsletters should be viewed only as recommendations, unless specific regulatory or statutory requirements are cited.*

Footnotes

1. https://csrc.nist.gov/publications/detail/sp/800-39/final