OCR Newsletter Addresses using HIPAA security measures to mitigate or prevent APT or zero day attacks

Advanced Persistent Threats (APTs) and Zero Day Exploits, alone or together pose dangerous threats to computers and data worldwide. This OCR Newsletter describes how the use of various HIPAA security measures can assist in mitigating or preventing damage caused by these types of cybersecurity attacks.

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.* These attacks are a serious threat due to the persistent nature and ability to change tactics in order to avoid detection. Such cybersecurity attacks pose a threat for any information technology (IT) system, but especially in the healthcare industry where APTs have been implicated in several worldwide healthcare sector cyberattacks.

In a zero day exploit or attack hacker’s take advantage of previously unknown hardware, firmware, or software vulnerabilities through research or probing or before a patch or anti-virus is made available to the public. Such exploits are more difficult to detect and increase the need for an overall security management process, including monitoring of anti-virus or cybersecurity software for detection of suspicious files or activity. In addition, appropriate safeguards, including encryption and access controls, may mitigate or even prevent unauthorized access to, or loss of, protected information.

Together APTs and zero day threats can threaten computers and data worldwide. For example, EternalBlue exploit targeted vulnerabilities in Microsoft’s Windows operating systems. Once public, the EternalBlue spread and infected other systems through the use of the WannaCry ransomware and infected hundreds of computers around the world resulting in billions of dollars in damages.

The HIPAA Security Rule sets forth the following security measures that can reduce the impact of an APT or zero day attack:

- 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)).