THE
NATIONAL LAW REVIEW

OCR Publishes Recommendations to Prepare for Cybersecurity Threats

Article By
Jennifer Orr Mitchell
Jared M. Bruce
Dinsmore & Shohl LLP
Legal News

- Health Law & Managed Care
- Insurance Reinsurance & Surety

- All Federal

Monday, April 8, 2019

The Department of Health and Human Services Office of Civil Rights (OCR) Spring 2019 Cybersecurity Newsletter includes new recommendations regarding how HIPAA covered entities can prepare to defend against cybersecurity attacks such as advanced persistent threats (APTs) and zero-day vulnerabilities. These cybersecurity threats were used by hackers in the global WannaCry ransomware cyberattack, which severely impacted the United Kingdom's National Health Service and several United States HIPAA-covered entities and business associates in May 2017.

According to the National Institute of Standards and Technology (NIST), an 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] APT attacks may not be as sophisticated as other hacking attacks, but the persistence of the attack and the capability for the attacker to change tactics to avoid detection makes APTs formidable threats to health care organizations. Health care data is particularly valuable to hackers who can use the information to blackmail an individual and compromise the confidentiality, integrity, or availability of the affected individuals' protected health information.

Zero-day exploits are cybersecurity attacks which attempt to exploit unknown hardware, firmware, or software vulnerability. Through research and probing, hackers can discover zero-day exploits in antivirus software and take advantage of the lag time between the discovery of the vulnerability and the availability and/or

implementation of the software patch or update. OCR states that these attacks are especially dangerous because their unique nature makes them more difficult to detect than ordinary hacking attacks. OCR emphasizes that HIPAA covered entities must be diligent in monitoring their cybersecurity or antivirus software for any unusual activity or suspicious files. Moreover, HIPAA covered entities should consider adopting other protective measures such as encryption, access controls, or network access limitations to mitigate the potential impact of zero-day vulnerabilities until a patch or upgrade is available.

OCR recommends that HIPAA-covered entities and business associates implement the following security measures contained in the HIPAA Security Rule (specifically the security measures set forth at 45 CFR § 164.308 and 45 CFR § 164.312) to proactively mitigate or prevent the harm that an APT or zero-day attack may cause:

- Conducting risk analyses to identify risks and vulnerabilities;
- Implementing a risk-management process to mitigate identified risks and vulnerabilities;
- Regularly reviewing audit and system activity logs to identify abnormal or suspicious activity;
- Implementing procedures to identify and respond to security incidents;
- Establishing and periodically testing contingency plans including data backup and disaster recovery plans to ensure data is backed up and recoverable;
- Implementing access controls to limit access to ePHI;
- Encrypting ePHI, as appropriate, for data at rest and data in motion; 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.

The full Spring 2019 OCR Cybersecurity Newsletter is available here.

[1] Available here: https://csrc.nist.gov/publications/detail/sp/800-39/final.