Report on Patient Privacy Volume 19, Number 5. May 08, 2019
OCR: Keep Watch Against Zero Day, APTs Attacks

By Theresa Defino

In its first cybersecurity newsletter of the year, the HHS Office for Civil Rights (OCR) is sounding an alarm to remind covered entities and business associates of some of the dangers that lurk in the technosphere: zero day threats and advanced persistent threats (APTs). Some have evocative names like WannaCry or EternalBlue.

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," OCR explains.

According to security experts, zero day refers to the lack of time (or days) that a software developer has to address a sudden vulnerability because it's already been exploited.

OCR calls zero day exploits or attacks "one of the most dangerous tools in a hacker's arsenal." When unleashed, the attack "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 are not the "standard" types of attack: by their nature, they're "more difficult to detect and contain than standard hacking attacks," says OCR. This is why "an organization's overall security management process" should include "monitoring of anti-virus or cybersecurity software for detection of suspicious files or activity."