Don't Let a "Man in the Middle" Monkey with Your Health Data

05.10.2017

There are numerous causes of breaches of protected health information (PHI), ranging from human oversights to “high-tech” errors. In April, the Office for Civil Rights (OCR) within the Department of Health and Human Services focused on the high-tech aspect of the equation, and warned against “man-in-the-middle” (MITM) attacks.[1] MITM attacks involve interception and infiltration of an online transmission by a third party, who may then infect, manipulate, or steal the transmitted data.

Secure Hypertext Transport Protocol (HTTPS) is a common security tool to protect communications sent via the internet. For example, you frequently may see the “https” designation when accessing websites that allow you to make financial transactions. The security of HTTPS can be evaluated using an “interception product,” which reviews and assesses internet traffic after decrypting it, and then re-encrypting it before sending it to its intended destination. Although these products are designed to root out malware, OCR identifies several key issues resulting from weaknesses in the products themselves or with their implementation. Such issues include failures to properly validate security certificates and failures to issue correct security warnings, which could negatively affect security of data transmission and lead to MITM attacks.

OCR is concerned about MITM attacks because the transmission of PHI can be vulnerable to such incidents. OCR highlights key resources for those who rely on HTTPS and interceptions products, including U.S. Computer Emergency Readiness Team (US-CERT) alerts, as well as the National Institute of Standards and Technology (NIST) SP-800 series guidance documents.

Entities subject to HIPAA may be familiar with NIST and its guidance documents, as OCR has promoted their use to understand and implement certain requirements of the HIPAA Security and Breach Notification Rules.[2] OCR also addresses in its guidance the role of risk analyses, an important Security Rule requirement, in evaluating HTTPS and interception products. As “high-tech” attacks become a more significant source of data breaches, covered entities and business associates must understand the technical aspects of, and obtain and maintain the security measures designed to prevent and mitigate, sophisticated malware and other cyberattacks.

[1] “Man-in-the-Middle Attacks and HTTPS Inspection Products,” *April 2017 Cybersecurity Newsletter*, Office for Civil Rights, April 3, 2017.
[2] 45 C.F.R. Parts 160 and 164, Subparts A and C; 45 C.F.R. 164.400 et seq.

Related People