COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 23, Number 12. December 07, 2023 OCR: Avoiding Security Rule Lapses Can Guard Against Common Cyberattacks

By Jane Anderson

Cyberattacks and ransomware demands have exploded in the health care sector in recent years, leading to multiple large breaches. But an analysis of those large breaches by the HHS Office for Civil Rights (OCR) has found common shortcomings that other organizations should address to prevent their own security incidents, a top OCR official said.

Nick Heesters, senior advisor for cybersecurity for the Health Information Privacy, Data, and Cybersecurity Division of OCR, said in a recorded webinar released Oct. 23 that proper implementation of HIPAA Security Rule provisions can help organizations prevent, detect, mitigate and recover from security incidents and breaches.[1]

The types of large breaches—those affecting 500 or more individuals—reported to OCR over the last five years have changed, Heesters explained. Breaches attributed to hacking or information technology (IT) incidents accounted for 49% of all large breaches cumulatively from September 2009 through December 2022; however, from January through September 2023, hacking and IT incidents accounted for 77% of all large breaches, he said.

Meanwhile, theft of devices containing protected health information (PHI)—which used to be far more common as a type of large breach—only accounted for 2% of all breaches in the first nine months of 2023, Heesters said.

"The big takeaway from this data is that a hacking breach is the most common type of large breach that a regulated entity is likely to experience," he said. "This is consistent with what OCR observed last year, where hacking was about 79% of the large breaches reported to OCR in 2022."

OCR has seen a 239% increase in large breaches involving hacking from 2018 to 2022, Heesters said, adding, "For ransomware, it's a 278% increase for the same time frame. This is the largest cybersecurity threat facing the health care industry and the protected health information it holds."

When it comes to the location of large breaches, data spanning the years from 2009 through 2022 shows that 31% of large breaches occurred in network servers, while 21% occurred in email systems, and 17% occurred in paper records, Heesters said.

For the first nine months of 2023, network server-based breaches were far more dominant, representing 67% of all large breaches, he said. Email system-based breaches fell slightly to 18% of all large breaches. Paper records represented only 5% of large breaches. "In sum, network servers and email accounted for 85% of the large breaches reported to OCR this year," he said.

Breaches Contain Common Threads

OCR investigations find "some commonality" in breaches resulting from successful cyberattacks, Heesters said. "Perhaps unsurprisingly, successful phishing attacks, attacks leveraging compromised credentials, and exploitation of unpatched vulnerabilities play a role in the initial attack vector or for a subsequent step to elevate privileges, access sensitive data—including PHI—and deploy malware," he said.

A typical ransomware attack consists of four phases, he said.

1. Initial intrusion, in which attackers gain entry to the system, device or file through malware infection.
2. Reconnaissance and lateral movement, in which attackers increase their knowledge of the environment and deploy ransomware across the network.
3. Data exfiltration and encryption, in which attackers exfiltrate data and lock the user out of the system, device or file.
4. Ransom demand, in which the device displays a message with a ransom note that contains the attacker's demands for payment.

OCR's investigations have revealed that the attacker typically gains access via a compromised nonadmin account, Heesters said. "This is sometimes due to compromised credentials or a successful phishing attack that captures credentials or deposits malware," he said, adding that the nonadmin account now under the attacker's control is used for reconnaissance and to deploy tools to discover vulnerabilities.

"Next, the attacker elevates privileges by exploiting vulnerabilities to compromise an administrator account such as a local or domain administrator or the root user of a Unix or Linux system," Heesters explained. "Finally, the attacker exfiltrates sensitive data—including PHI—deletes backups and deploys malware, typically ransomware, but may include backdoors to try and maintain access to compromised systems when discovered."

An attacker can gain a foothold in an organization's information systems through a variety of means, he said, and a popular vector is leveraging compromised credentials to access a system remotely.

OCR investigations and subsequent analysis found that single-factor (e.g., password) remote access and poor password rules provided opportunities for attackers to gain access to nonadmin accounts, Heesters said. "A popular password strength chart estimates that passwords with a length of four or five characters, regardless of complexity, can be cracked using brute force methods almost instantly," he said. "In addition to password length, poor passwords generally were found in various investigations, including passwords that were the same as the user ID, oftentimes on service or application accounts, such as a test or software account."

Default passwords—such as those that come preconfigured on devices for administration and configuration—also were observed, he said. "Some investigations found entity default passwords in use that were included in manuals available on the internet or circulating online in hacker forums."

In addition, entities using anonymous file transfer protocol (FTP), a configuration of FTP requiring no authentication, also were identified during several investigations, Heesters said, adding, "at least one entity relied on anonymous FTP for clients to upload logs for software diagnosis, but these logs contained PHI."

The HIPAA Security Rule includes a requirement for authentication: implemented procedures to verify that a person or entity seeking access to electronic PHI (ePHI) is the one claimed, Heesters said. "Access to ePHI with no authentication via anonymous FTP, or even with authentication but using weak authentication rules and solutions such as four- or five-character passwords, does not ensure the confidentiality, integrity and availability of ePHI," he said.