Report on Patient Privacy Volume 22, Number 2. February 10, 2022 'Zero Trust' Offers Promise of Defense Against Stolen Credentials, Ransomware

By Jane Anderson

A security architecture based on a concept called "zero trust" holds the potential to defeat the current scourge of cyberattacks and ransomware plaguing health care organizations. However, implementation requires significant resources, buy-in from top management and a step-by-step approach with constant communication to end users, according to cybersecurity experts.

"Today, 80% of all attacks involve the use of legitimate network credentials," said Drex DeFord, executive health care strategist at CrowdStrike. In organizations that have not implemented zero trust, "such cybercriminal access appears to be completely normal. Threat actors using those credentials are allowed to move from one part of the network to the next. They can download private data, identify a broad spectrum of weaknesses in networks and applications, and lay the groundwork for ransomware attacks, all without being detected."

Key to the zero trust architecture is requiring all users, whether in or outside the organization's network, to be authenticated, authorized and continuously validated for security configuration and posture before being granted or keeping access to applications and data, DeFord said. "The solution should enforce consistent risk-based policies to automatically block, allow, audit or step up authentication for every identity, all while ensuring a frictionless login experience for genuine users," he said.

"These policies are defined and enforced in real time, based on authentication patterns, behavior baselines and individual risk scores to verify identities using step-up authentication such as multifactor authentication," DeFord explained. "This approach automatically resolves security incidents that the user approves using identity verification methods such as [multifactor authentication], without involving security analysts and/or help desk tickets. This sounds difficult, but it's made way easier today by advanced tools and services from leading cybersecurity partners."

DeFord and other cybersecurity experts shared their thoughts on zero trust with *RPP*, detailing what zero trust means, how it can be implemented, and the benefits it could bring to health care organizations that are covered by HIPAA.