COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 22, Number 2. February 10, 2022 Steps to Implement 'Zero Trust'

By Jane Anderson

The first step for health care organizations that want to implement zero trust is to identify which applications and users to protect, and to take a one-app-at-a-time approach, explained Den Jones, chief security officer at San Francisco-based zero trust access solution firm Banyan Security.

"Zero trust implementations result in something we call user-to-application segmentation, which simply means we're pairing specific users to specific applications," Jones said. "So when zero trust is done right, you can deploy it incrementally rather than having to perform a gigantic rip-and-replace of your legacy VPN [virtual private network], for example. That way, you reduce risk and assure yourself that the new system is working before removing access to any old systems. Once you have success applying zero trust to one application, you can then identify your next one, and so on," he explained.

Jones, along with Chuck Everette, director of cybersecurity advocacy at advanced artificial intelligence security company Deep Instinct, and Drex DeFord, executive healthcare strategist at CrowdStrike, offered more advice on implementing zero trust within a health care organization:

- Make sure to understand what a zero-trust framework is (and isn't), Everette said. "Organizations do not always have a clear definition or understand the value of a zero-trust business model. Educating that shift to a zero-trust framework is a cultural change and transformation. You have to build advocacy, support and budget expectations from the very beginning. Having key stakeholder engagement and company-wide buy-in and acceptance is critical."

- Do the work to get executive buy-in, Jones said. "Help them understand that there are both security and useability benefits. The right executive sponsor can really be the difference between project success and failure." Keep key stakeholders updated on expectations and progress, Everette said, adding that "stakeholders can make or break your effort."

- Resist the urge to settle for "good enough" cybersecurity, DeFord said. Artificial intelligence/machine learning solutions should serve as the foundation for zero-trust security solutions, he said.

- Cultivate a full understanding of the tactics, techniques and procedures (TTPs) adversaries use, DeFord said. "Security teams need to stay up to date with the latest TTPs, as adversaries constantly change their tradecraft to attain access," he said. "Security teams that gather this intel in real time," and have the support of artificial intelligence/machine learning solutions, "can leverage this intel and are in the best position to defend against adversaries in real time."

- Allow for adequate time to learn the new way of doing things, since change is hard for people, Jones said. Still, make sure you implement boundaries and limits as to how long to permit the "old way" to be used, he said.

- Communicate to the point of overcommunicating, Jones said. Make certain no one is surprised about what is happening, why it's happening and when it's happening. "It's amazing how often this important subject

is neglected," Jones said.

- Ensure that basic security hygiene is in order, disabling any unused accounts such as generic, vendor or application programming interface accounts that often are forgotten, Jones said. When reviewing application access, pay attention to things that people have access to but haven't used or don't need, possibly because they changed roles. "Continuously removing access to applications and services that haven't been accessed in 90 days is also a great practice whether you're using zero trust or not," Jones said.
- Find an ally to advise you. "It might be a vendor, but it can also be a peer who's already been down the path," Jones said.
- Finally, don't fall for common zero trust myths, such as "zero trust creates a bad user experience," or "zero trust means you do not trust your staff, employees or clients," Everette said.

"Zero trust isn't about buying or deploying a product; it's first and foremost about making conscious decisions about your security strategy," Jones said. "Examine your identity, multifactor authentication and endpoint systems to make sure you're getting benefit from the technology you've already deployed. Any new zero trust system should leverage the tech stack you already have."

Contact Jones and Everette via Katie Brookes at brookes@merritgrp.com. Contact DeFord via Webbo Chen at webbo.chen@crowdstrike.com.