How to Secure Your Network Identities

An interview with **Alexandra Weaver**, Senior Solution Architect, Semperis

Cloud computing has dramatically changed how agencies offer services, much like smartphones have transformed how people access and use information. But these new data-sharing opportunities create new identity-related risks.

"Think of the old-school pictures where you had a [physical] data center," said Alexandra Weaver, with Semperis, a firm that provides comprehensive identity protection. "That really isn't the case anymore with the cloud. We have all these offerings that are everywhere, and … we need to [say], 'Hey, what am I now protecting? Well, I'm now protecting my identity.'"

It's the new network perimeter, she explained. But despite the importance of safeguarding it, organizations often struggle to make the transition.

Friction Is Real

"There's going to be friction when [agencies] change processes," Weaver said. "A lot of these agencies have been doing solid work … for years and transforming becomes difficult."

In fact, legacy applications and technology are often the babies that agencies have proudly nurtured for decades. Speaking from personal experience, she said there can be emotional ties to old IT that someone has "kept solid for [the] environment" for years.

It's important to have an industry partner, such as Semperis, that can talk early on about future efficiencies and other benefits and include agency staff in designing new workflows. "Building team camaraderie in the decision-making process is important from the beginning," Weaver said. "It's having everyone together at that table, defining their goals and aligning them and making sure that we're meeting their business outcomes."

Suite of Services

Semperis gives agencies visibility into their environment's security and helps make them proactive instead of reactive. A full product suite offers tools for before, during and after a cyberattack, Weaver said.

That includes continuously scanning an agency's Active Directory for vulnerabilities, monitoring for indictors of exposure and compromise, and having uninterrupted visibility into attacks other monitoring tools can't see.

The platform automatically remediates breaches when waiting for human intervention would be too risky and gives real-time threat notifications.

In the event of a cyberattack, Semperis has a two-pronged approach to restore the system, said Weaver. First, identify what happened, go step by step to look for loopholes and hidden objects, backdoors that the attacker might have created and, second, restore to a trusted state.

Restoring data is harder when an agency turns to Semperis only after an event. "A lot of [agencies] won't have the internet, so I helped one organization while they held up their cellphone so I could see their screen," she recalled.

Purple Knight

Developing a baseline understanding of your system's vulnerabilities is the first step to a strong cyber defense. Running Semperis's Purple Knight on a network computer is one option, Weaver said. "No elevated permissions, no superpowers, just a regular user on a computer" can do it, she said.

The free tool scans an agency's system, identifies weaknesses, assigns a vulnerability score and offers prioritized guidance.

"With all of the threats that exist today, we have to be one step ahead," she said.