FORTINET FEDERAL

The Human Side of Zero Trust

The May 2021 Executive Order on Improving the Nation's Cybersecurity (cyber EO) came on the heels of high-profile cyberattacks that plagued public and private sector organizations, including the Colonial Pipeline attack that caused gas shortages along the East Coast. The Colonial Pipeline attack was perhaps the most tangible example yet of how a cyber incident can affect government, industry, and individuals.

The sweeping cyber EO that followed included 11 sections of guidance and mandates designed to push Federal agencies to improve their cybersecurity posture and modernize their infrastructure. Many of the mandates involve building a zero trust architecture, which requires users and devices to be authenticated and authorized before accessing the agency network, applications, and data.

"The cyber EO brought people together in a shared mission," said Jim Richberg, public sector CISO at Fortinet.

"[It] really got Federal agencies and the vendor community aligned on technology solutions in a way that we typically haven't seen in government," said Richberg. "The government quickly put out a strategy, technical reference architectures, a maturity model, and shared capabilities information to guide agencies on the path to implementing zero trust principles, which also guided the vendor community."

Paying Attention to People Alongside Processes and Technology

Implementing a zero trust architecture involves people, processes, and technology. People – especially end users – are a vital element of the zero trust equation, but they are often overlooked in the rush to meet mandates. "That's a mistake," Richberg said.

"The label 'zero trust' can have Orwellian connotations of surveillance and distrust that are especially off-putting to workers focused on public services, many of whom have security clearances," he noted. "Those of us who work with zero trust principles every day know what it means, but for the end user who may not, zero trust sounds like 'I don't trust you.' They may consciously or unconsciously push back. In essence, the government has a branding problem when it comes to zero trust."

The concepts behind zero trust are no different than the metal detectors and access badges that are standard across Federal office buildings, observed Felipe Fernandez, senior director, system engineering at Fortinet Federal. "People don't think twice about having their bags screened in the lobby or using their badge in the elevator to access the floor where their office is located," he said. "That is zero trust – you are being checked and verified at various entry points to ensure you don't pose a risk and that you have the proper credentials."

Explaining zero trust in clear terms and showing how it can provide the capabilities to enable work from anywhere and provide a safety net to minimize the consequences of user error can go a long way toward making the concept more user friendly and easing its adoption in the workplace, Richberg advised.

"Instead of zero trust, it can be explained in a way that says, 'We trust you to go where you are authorized to go,'" he added.

Building a zero trust mindset in the workforce should be a priority as agencies work to meet the zero trust mandates, Fernandez said. "By helping users understand the need for cybersecurity – just like there is a need for metal detectors – they can become allies," he added.

Addressing Workforce Gaps

The IT workforce is another vital element of the zero trust equation. Building an integrated zero trust architecture is a holistic process rather than a single upgrade, but technology teams that are experiencing workforce shortages may feel like they don't have the time or resources to build an integrated solution.

However, the approach to zero trust outlined in the cyber EO can help alleviate some workforce stresses, said Peter Newton, senior director, product marketing, at Fortinet. "It gives technology teams a singular focus. There is little room to get distracted by shiny new tech or the latest security capability," he said.

Zero trust is designed to be outcome focused, not capability focused, which will help overcome the cybersecurity skills gap, Fernandez noted, because a zero trust architecture doesn't require a subject matter expert for each capability. Instead, a few staff can ensure the various technology components are working properly, while everyone understands the outcomes of the holistic implementation.

In addition, "implementing zero trust means creating automations, which reduces time spent on manual processes," Newton noted, so tech talent can be redeployed to support mission goals.

Aligning Zero Trust to the Mission

The Zero Trust Maturity Model released by the Cybersecurity and Infrastructure Security Agency (CISA) helps agencies prioritize the work of building zero trust security based on the components they already have in place. To fill in the gaps, agencies can then decide to follow a specific zero trust framework that aligns with their situation and mission. For example, an agency could choose to follow the zero trust framework from CISA, the Defense Department, the National Security Agency, or the National Institute of Standards and Technology.

"This flexibility means zero trust won't be an incomplete experiment," Fernandez said, "because now, any agency has the flexibility to choose a zero trust model that's appropriate for its needs, instead of being stuck with a framework that doesn't flex to address its use cases."

FORTINET FEDERAL®