Executive Order on Improving the Nation's Cybersecurity — Ushering in a New Age of Security

This Executive Order makes clear that modernizing our current digital situation is a moral imperative and that failure is not an option.

Sean Frazier
Federal CSO
Okta

President Biden took a major step forward in ensuring that the U.S. government has the resources and focus needed to address our cybersecurity needs with the issuance of Executive Order on Improving the Nation's Cybersecurity. This focus is long overdue. For nearly a decade, we've lived in this tenuous world where the next critical cyber event lies just around the corner, but the seeds were planted long before that.

The day we decided to connect our agencies or our enterprises to the larger network (the Internet), the risks became significantly higher. And now, more than ever, we see attacks like with Solarwinds come along and realize that this is not the end but really only the beginning. We find ourselves wondering if we'll ever be truly safe from attackers in this modern, very digital, very connected world.

Well, it finally looks like, from a government perspective, we are starting down the right path. This EO—which promotes Zero Trust, enhanced endpoint protection, multi-factor authentication, and software development standards—will serve as the initiation of a long-needed shot-in-the-arm for focusing our attention on the ever-increasing threat. It has placed much-needed awareness and focus on true threat mitigation.

Let's face it: we've made it too easy on the attackers. They keep hitting targets with the same tried and true methods of attack (phishing, credential-based attacks, etc.), and yet in the press and in our lives, we tend to spend time talking about "zero-day" attacks and attacks that are novel and sophisticated.

Novel and sophisticated attacks cost time and energy for attackers. But think of our adversaries as business folk, running a business. Why would they focus on very expensive, very limited attack vectors when they have a low-cost, high-success-rate alternative? It doesn't matter what their motivations are—whether financial or political. If they can "do more with less," why wouldn't they? If they could gather and use valid credentials to leverage a valid-looking access flow, that's the path of least resistance. Their business is just like yours; if they see a path with a better ROI, they will certainly pursue it.

This new directive makes clear that modernizing our current digital situation is a moral imperative and that failure is not an option. It also makes it clear that digital modernization or transformation most often takes the form of cloud adoption or the adoption of cloud services to deliver capability.

Many folks out in the world, myself included, have been preaching the benefits of adopting a Zero Trust "mindset" for some time now. This mindset includes providing protections for the most vulnerable attack

Many are advocating the benefits of adopting a Zero Trust "mindset". This mindset includes providing protections for the most vulnerable attack surface (the password) by building systems that utilize Single Sign-on (SSO) and strong Multi-factor Authentication (MFA).

surface (the password) by building systems that utilize Single Sign-on (SSO) and strong Multi-factor Authentication (MFA).

For too long, we've put much of the security burden on the end-user (passwords) without giving them the proper protections for these arcane constructs. This EO shines a light on this oversight and requires us to do better.

The EO also brings cloud modernization into the right area and delivers it through the FedRAMP program, which makes total sense. The FedRAMP program was designed specifically to reduce and manage risk (heck, it's in the name!) and to enable modernized, cloud-based services to become the vehicle for change that most of us knew it could be.

One of the historical problems with the FedRAMP program, while very popular and very successful, is it also becoming a bit of a bottleneck because of its success and popularity. Now that we are thinking about cloud and cloud security as top priorities, the FedRAMP program needs its own funding stream and needs to be a first-class delivery program.

Congress has sought to address this through legislation via HR 21: the FedRAMP Authorization Act of 2021, which was the very first bill passed by the 117th Congress. Enacting this legislation into law, combined with what's required by the executive order, provides a foundation to do cloud security the right way. Now, we just need to match the investment with the promise.

Learn more at www.okta.com. ■

About The Author

Mr. Frazier is Federal CSO at Okta. In his role, Sean acts as the voice of the CSO for Okta's federal business. Prior to joining Okta, Sean spent more than 25 years working in technology and public sector security for companies such as Duo Security, Netscape, LoudCloud/Opsware, Proofpoint, Cisco & MobileIron. Sean has helped lead numerous projects used by the Department of Defense and Intelligence Community, including the Fortezza Crypto Card, Defense Messaging System (DMS) and many others. He also has extensive experience in identity and public key infrastructure (PKI), network, applications, mobile and IoT. Sean has testified in front of the U.S. Senate Homeland Security and Government Affairs Committee on the importance of public/private partnership in protecting the nation's digital infrastructure. Sean also advises public/private partnership working groups including ACT-IAC, ATARC and many others.