Galvanizing agencies into action on cybersecurity

Recent directives have given agencies the guidance they need to develop a more robust, layered security architecture

Nick Heudecker

Cribl

The Executive Order on Improving the Nation's Cybersecurity has spurred agencies to modernize the way they protect IT systems and data. Now there is a shared commitment to the steps that IT leaders should take, and agencies have been galvanized into action.

For example, zero trust was mostly just a buzzword for agencies prior to the executive order, and now it is something that federal agencies are seriously exploring. They're going beyond reading whitepapers to asking for vendor demos and testing ideas. In addition, supply chain security and endpoint detection and response are now top of mind for many agencies because of the executive order's emphasis on those activities.

Collaborating on cloud security

One important offshoot of the executive order is the Office of Management and Budget's maturity model for event log management, which defines the proper formatting and use of timestamps in event logs. Having a cohesive data format goes a long way toward enabling non-experts to understand event logs, and it enhances the shareability of data between agencies and with the Cybersecurity and Infrastructure Security Agency. The ability to route data to many places amplifies the value that can be derived from that data — for insight into current security events, for future research and for regulatory compliance.

Cloud security is another key focus of the executive order. Agencies often find that cloud-native security controls are not as robust as their on-premises tools and may only cover certain aspects of application, data or network security. In addition, when the cloud operations team uses cloud-native controls without involving the security team, that lack of coordination can have serious ramifications, especially in multi-cloud environments. Therefore, agencies may need to focus on ensuring more collaboration between the cloud operations and security teams for more complete security coverage.

Agencies also have to figure out how to integrate multi-cloud security capabilities without hampering their application developers. This is where the use of DevSecOps comes in handy.

Easing the security burden for agency employees

Modernizing and maintaining security is a tremendous burden for an agency's staff, especially because security professionals are in short supply. The situation will continue to worsen as the cyberthreat landscape becomes more complex.

There are a number of ways that agencies can ease that burden. A cloud security posture management, or CSPM, product can help automate security and correctly implement policies across multiple cloud environments, and third-party virtual appliances can secure north-to-south as well as east-to-west network traffic.

Joel Filipe

> Security can break down even on a simple upgrade cycle, so it takes a conscious commitment to **maintain that momentum and ensure ongoing protection.”**

Agencies may also want to consider creating a physical point of presence for additional layers of security, particularly in hybrid environments that include on-premises systems, to ensure that everything is secure according to federal mandates and regulations.

In addition, agencies should plan to invest heavily in skills and training for multiple cloud platforms in a hybrid environment. Security is an iterative process that requires organizations to be continuously adaptable. By training employees on the latest and greatest security capabilities, they will know what’s possible and how to achieve it.

In general, the executive order has forced federal IT leaders to act and given them specific directions on how to develop a more robust, layered security architecture. Agencies will need to continue that work to ensure that the improvements don’t fall by the wayside, especially in areas that involve collaborating with other federal entities. Security can break down even on a simple upgrade cycle, so it takes a conscious commitment to maintain that momentum and ensure ongoing protection. ■

Nick Heudecker is senior director of market strategy at Cribl.