CREATING A BLUEPRINT FOR CLOUD SECURITY

Government efforts to construct secure cloud environments have intensified during the coronavirus pandemic

GOVERNMENT OFFICIALS NATIONWIDE had to hit the fast-forward button on modernization initiatives to ensure that teleworking employees could access networks and data from remote locations. For many agencies, that meant a higher reliance on cloud technology and a possible expansion of their cybersecurity vulnerabilities in an environment already attractive to hackers.

Agencies had been increasing their use of cloud technology before the COVID-19 outbreak. Over the years, cloud adoption was spurred by the Obama-era Federal Cloud Computing Strategy (popularly known as Cloud First) and the Trump administration's update of that strategy, called Cloud Smart.

The policy emphasis is having an impact. According to research conducted by IDC on behalf of Thales, 54% of federal government data is now stored in the cloud, surpassing private-sector cloud adoption. Furthermore, federal agencies estimate that 51% of the data they store in the cloud is sensitive.

Although many experts say cloud environments can be more secure than on-premises systems, they're far from immune to vulnerabilities. On March 13, as agencies began shifting to telework in response to the coronavirus pandemic, the Cybersecurity and Infrastructure Security Agency (CISA) warned agencies to be prepared for an increase in phishing attacks on teleworkers and encouraged agencies to use multifactor authentication.

Two months later, CISA issued an alert stating that advanced persistent threat groups were targeting organizations involved in pandemic response, including local governments and health care entities.

Guidelines for structuring cloud security

In response to the security challenges raised by the cloud, the federal government has provided myriad foundational documents, guidelines and strategies to help agencies create a strong security posture, which is not always straightforward given the mix of on-premises, private and commercial cloud environments that many agencies use.

Most notably, the Federal Risk and Authorization Management Program (FedRAMP) provides a standardized approach to assessing, authorizing and continuously monitoring cloud services and products. FedRAMP ensures that agencies have access to cloud technology that meets the government's rigorous standards and has encouraged providers to raise their own standards.

Furthermore, security is one of three main pillars of the Cloud Smart strategy, which reinforces a call for agencies to use "data-level protections and fully leverage modern virtualized technologies." It states that "encryption and [identity, credential and access management] implementation is particularly relevant in the context of cloud-based environments, namely in those instances where an agency is partnering with an external service provider to manage network visibility and data protection."

The Cloud Smart strategy also recommends service-level agreements that give an agency "continuous awareness of the confidentiality, integrity and availability of its information" and notes that the governmentwide Continuous Diagnostics and Mitigation program "continues

Gluiki/Shutterstock/FCW Staff

CLOUD SECURITY BY THE NUMBERS

$7.1B

Amount federal cloud spending is projected to reach in 2020

$9.1B

Amount federal cloud spending could reach in 2024

45%

Agencies that use private clouds

17 of 22

Number of action items that have been completed under the Cloud Smart strategy

Sources: Bloomberg Government, CIO Council, Deltek, FCW

to evolve so that agencies are equipped with the monitoring capabilities they need to understand their cyber risk in the cloud."

Fortuitously, the government released draft guidance on an updated Trusted Internet Connections (TIC) initiative near the end of 2019. TIC began more than a decade ago as a way to limit the number of agency connections to the internet, which made sense at the time. But networks and security have evolved in the intervening years, so TIC 3.0 includes cloud as an official use case, making it easier for agencies to adopt the technology.

In response to the coronavirus lockdown, CISA specifically references TIC 3.0 in the telework guidance released on April 1. The goal is to provide "security capabilities for remote federal employees securely connecting to private agency networks and cloud environments."

Cloud security is top of mind for state and local government leaders, too. The 2020 list of the top 10 priorities for members of the National Association of State CIOs includes cybersecurity and risk management at the top and cloud in third, just behind digital government — in terms of strategy, policy and management. However, when it comes to technologies, applications and tools, the No. 1 priority is cloud solutions (specifically software as a service).

The need for a more modern approach to IT systems was apparent this spring when several states — including Connecticut, Kansas and New Jersey — put out a call for Cobol programmers to help with systems running on decades-old mainframes that teleworkers couldn't access.

The lasting impact of the pandemic

Cloud technology has a crucial role to play in agencies' ability to modernize IT systems and take advantage of the latest technological innovations. Because of its importance, cloud adoption must keep pace with security efforts. For example, despite the fact that the Office of Management and Budget requires agencies to use FedRAMP to authorize the use of cloud services, 15 of 24 agencies recently surveyed by the Government Accountability Office said they did not always use FedRAMP. Specifically, agencies reported using 247 cloud services that had not been certified. GAO recommended that OMB enhance its oversight and that the General Services Administration, which manages FedRAMP, improve its guidance and monitoring.

Still, more than half (58%) of respondents to a recent survey of FCW readers said the security of cloud-based technology is a top priority, and 83% said their agencies have strategies for managing compliance with various security standards in the cloud.

The response to the coronavirus pandemic has demonstrated that agencies can continue to function when most employees are teleworking, and in many ways, cloud-based technology has enhanced teamwork and productivity. Some of those changes may be here to stay. Fortunately, security approaches are evolving to better fit today's networking realities, and the stage is set to ensure that those changes aren't just functional but are also secure. ■