Building a Resilient Cybersecurity Organization in Government

Before they migrate to cloud, government agencies need a strong security architecture.

Government agencies are moving to the cloud. According to a Center for Digital Government (CDG) survey, most agencies now run an average of two to five clouds. At the same time, there are an estimated 80,000 cloud applications available to government today.

Cloud offers many advantages, but it can also present risks if an agency doesn't carefully consider the security aspects involved in migrating from an on-premises environment to the cloud.

"We have clients that want to move from no cloud implementations to 95 percent cloud in two years," says John McLaughlin, Executive Cyber Security Architect for IBM Federal. "That is fraught with risk. Before agencies make the leap, they need to conduct a security assessment and develop a well-thought-out security strategy."

"We have clients that want to move from no cloud implementations to 95 percent cloud in two years. That is fraught with risk. Before agencies make the leap, they need to conduct a security assessment and develop a well-thought-out security strategy."

— John McLaughlin, Executive Cyber Security Architect, IBM Federal

There are two primary types of cloud security. The first type is provided by the cloud vendor as part of the cloud deployment. The second type includes any security constructs built by the government agency — workload visibility, data protection and access control, for example — that add additional security protection to the cloud environment. This paper examines the latter and offers security recommendations for three cloud adoption patterns: Migrating on-premises workloads to the cloud, building cloud-native applications and migrating on-premises databases to a hybrid cloud environment.

Migrating On-Premises Workloads to the Cloud

An agency that plans to migrate on-premises workloads to the cloud should take steps to ensure its security plan is up to par. McLaughlin recommends the following:

1. **Conduct a thorough security assessment.** The assessment should focus on data and application security as well as compliance.

2. **Ensure security is up to date and optimized in three key areas.** The first area is access management — the process by

which individual users or government agencies access software applications within the cloud. This includes the portal third-party business partners use to access government applications. The second area is data protection. Insider threats are among the biggest risks to government security, so providing additional security practices inside the organization is critical. The third element is network protection. For example, ensure you have a strong white list. If a rogue piece of hardware is connected to your network, a good white list will enable you to quickly identify and isolate that piece of hardware until you can assess the risk.

3. Fine tune your threat management strategy. Ensure you can accurately and promptly put appropriate security practices in place if a network anomaly is detected.

Building Cloud-Native Applications

If your agency plans to use cloud-native technologies to develop cloud applications using containers, microservices and/or DevOps processes, keep these security steps in mind:

1. Implement API security. API security entails authenticating programs or role-based access control to ascertain whether an individual should have access to certain applications.

2. Leverage data encryption. It's critical to ensure you protect data that is in transit as well as data at rest. Also be sure that all encryption keys are up to date.

3. Continually scan the network to provide a holistic and comprehensive view of vulnerabilities. Monitor log and network flows consistently and merge those information flows into a single view of your security landscape. Ensure your security efforts are integrated with the enterprise security offered by your cloud provider so the two form a happy marriage dedicated to comprehensive, consistent data protection.

4. Develop and test an incident response plan. It's important to have a procedure that can be put in motion immediately should anything go wrong.

Extending an On-Premises Database to the Hybrid Cloud

Hybrid cloud means agencies can benefit from an integrated on-premises and cloud environment. But a hybrid cloud environment can create challenges when it comes to developing a consistent security environment and avoiding duplication of work. To ensure a secure hybrid environment, McLaughlin suggests agencies do the following:

1. Fully evaluate data protection efforts. This should include data discovery, classification and monitoring.

2. Develop access management and governance policies. Each of the major cloud vendors has a distinct advantage. The ability to handle more than one cloud vendor at a time is critical, and that will require good governance policies.

"The governance side is often underestimated in terms of time and effort," says McLaughlin. "A cloud security governance board should look at identity governance, privileged identity management, who accesses software applications and how they are accessed."

3. Take a holistic approach to monitoring and compliance. "There are five things you need to worry about when it comes to security: People, places, things, time and money," says McLaughlin. "You need to figure out how you're going to institute controls to ensure those five elements are correctly controlled within your security environment."

An estimated 25 to 30 percent of government budgets are spent on regulation and compliance reporting. A holistic approach can help you decrease those costs by reducing duplicate efforts and enabling you to see any security holes that need to be plugged.

4. Develop a roadmap. Asses where you are today and where you want to be in the future. Then develop a security roadmap for how to get from your current state to the desired state.

"A roadmap is key to cloud security success," says McLaughlin. "A government organization without a roadmap is like a chimpanzee with a chainsaw. There's a lot that's going to happen and none of it is good."

This information is part of the IBM Government Cloud Virtual Summit, a free, online event featuring 17 sessions with insightful keynotes, illustrative case studies and deep dives into job-critical topics for government leaders. To view any of these sessions, visit www.govtech.com/ibmvirtualsummit