Technology Strategies Notes

Volume 2, Issue 5
May 2015

Office of Technology Strategies (TS), Architecture, Strategy & Design (ASD)

A VA Executive's Guide to Cloud Computing: Cloud Privacy & Security

INTRODUCTION

In a previous TS Note (Volume 2, Issue 3, A VA Executive's Guide to Cloud Computing), we examined cloud computing, the main benefits that organizations like VA can gain from it, and a number of the current challenges that these organizations face when adopting a cloud services. Having previously introduced the basics, this TS Note will delve deeper into a subtopic of cloud computing, specifically covering data privacy and security in a cloud computing environment.

Cloud computing can have many positive effects on organizations, such as reduced operating costs, increased organizational elasticity, and greater service availability and reliability. Concerns about data security and privacy in a cloud computing platform, however, are regarded by many as one of the most significant barriers to the adoption of cloud services.

OVERVIEW

As discussed in A VA Executive's Guide to Cloud Computing, cloud computing is generally defined as a type of computing that relies on sharing computing resources rather than using local servers or personal devices to handle applications. By leveraging this technology, organizations can realize benefits like increased operational efficiency and improved service delivery. Current cloud services pose an inherent challenge to data privacy and security, however, because they typically result in data being present in unencrypted form on a machine owned and operated by a third-party organization. Concerns frequently arise over whether or not to trust the cloud service provider with this data, what the cloud service provider is technically allowed to do with the data once it is in their possession, how safe the data is from external attacks, and what level of control the data's owner should exercise on the data.

In a report that reflected the consensus among surveyed industry experts, the Cloud Security Alliance (CSA) identified the top nine cloud computing threats of 2013. According to CSA, the number one and two threats in the industry were data breaches and data loss, respectively. Permanently losing data is terrifying for any organization, and for those with sensitive internal data or PII/PHI, a data leak is catastrophic. The third greatest cloud computing security threat is account or service traffic hijacking, where a hacker plants a bug that hijacks users' account credentials, giving the hacker access to critical areas of deployed cloud computing services where they can launch more elaborate attacks.

SERVICE PROVIDER DILEMMA

Cloud computing poses privacy concerns because the service provider can access—and accidentally or deliberately alter or delete—the data that is on the cloud, if it is not encrypted. According to CSA, the threat level of "malicious insiders" is a true point of contention in the cloud security industry, although they do recognize it as a top risk. The degree of exposure to a third-party cloud services vendor and their other clients, however, is largely dependent on the model used to deploy the cloud computing platform. The National Institute of Standards and Technology (NIST) has identified four deployment models for cloud computing platforms:

- Private cloud: The cloud infrastructure is provisioned for exclusive use by a single organization and is managed by the organization or a third party. The infrastructure may be exist in-house or off-site.
- Community cloud: The cloud infrastructure is provisioned for exclusive use by a specific group of several organizations for supporting a specific community that has shared concerns. The infrastructure may be managed by the organizations or a third party and may exist in-house or off-site.
- Public cloud: The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated off-site by a third party.
- Hybrid cloud: The cloud infrastructure is a composition of two or more distinct cloud models that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability.

Many organizations work with third-party cloud service providers because they themselves do not have the resources to establish the same level of security, scalability, and cloud management expertise that third-party vendors have amassed.

The Notorious Nine: Top Threats in Cloud Computing in Recent Years

1. Data Breaches
2. Data Loss
3. Account or Service Traffic Hijacking
4. Insecure Interfaces and APIs
5. Denial of Service
6. Malicious Insiders
7. Abuse of Cloud Services
8. Insufficient Cloud Vendor Due Diligence
9. Shared Technology Vulnerabilities

Technology Strategies

Defining OI&T's "To Be" Technology Vision

The TS office within OI&T's Architecture, Strategy & Design (ASD) interacts with the ASD pillar offices, multiple stakeholders within OI&T, and strategic offices across the enterprise. TS works closely with IT and business owners to capture business rules and provide technical guidance as it relates to Data Sharing across the enterprise, specifically for interagency operability.

Continued on Page 2

Technology Strategies Notes

Volume 2, Issue 5
May 2015

A VA Executive's Guide to Cloud Computing: Cloud Privacy & Security

Continued from Page 1

Security in the cloud is achieved, in part, through third-party controls and assurance much like in traditional outsourcing arrangements. Additional challenges are associated with these arrangements, however, because there is no common cloud computing security standard. Many cloud service providers implement their own proprietary standards, security technologies, and distinctive security models, which need to be evaluated individually. In a vendor cloud model, it is ultimately up to client organizations to ensure that security in the cloud computing environment meets their own security requirements by gathering as many vendor risk assessments, due diligence, and assurance activities as possible.

AREAS FOR SECURITY CONCERNS

As shown in Figure 1 below, there are six specific areas of the cloud computing environment where industry experts claim that equipment and software require substantial security attention.

- Encrypting the data is one way for organizations to secure (1) data at rest and (2) data in transit from prying eyes, but if they lose the encryption key, the information will be permanently inaccessible.
- Strong (3) authentication protocol for users, applications, processes, and devices is crucial in any cloud deployment.
- Typically, a cloud provider would use virtual machines and a hypervisor to ensure (4) robust separation between data belonging to different customers.
- Each customer should have its legal and regulatory experts inspect cloud provider's policies and practices to guarantee that they are strong enough to address (5) cloud-related legal and regulatory issues. The issues to consider include compliance, auditing, and legal discovery.
- Finally, customers need an (6) incident response plan for the possibility of cloud provider security breaches or user misbehavior.

CLOUD SECURITY AND THE IT VISION

One of the core components of VA's IT Vision is access to cloud services, which is managed by a single sign-on capability. In this model, a VA user's credentials are passed along as they traverse the VA infrastructure and will allow them access to services and data authorized for each user. There are three levels of secure access to cloud applications:

- Low: Applications governed by access control policies that do not have strict role-based requirements about who can access data.
- Medium: Applications with basic role-based access aligned to specific roles which make data available only to the roles that are allowed visibility of that data.
- High: Applications with very tight security controls that protect sensitive information such as personally identifiable information (PII) or personal health information (PHI) and manage the authorization to access that information.

VA is actively establlishing long-term strategies and governance mechanisms to ensure that all cloud services comply with the latest Federal standards and are properly integrated into the IT infrastructure. Specifically, VA is completing a Cloud Security Handbook as part of the "Cloud First" policy (VA Directive 6517), and it requires all cloud services that have business agreements with VA to be accredited by a process known as the Federal Risk and Authorization Management Program (FedRAMP). Accredited cloud services connect to VA through standardized network access points that are managed continuously by the VA Network and Security and Operations Center (NSOC). This will help ensure that all cloud services meet the rigorous security and privacy standards that are needed to guarantee high-quality service to VA customers.

If you have any questions about cloud computing privacy and security, don't hesitate to ask TS (askTS@va.gov) for assistance or more information.

Check out earlier TS Note editions here

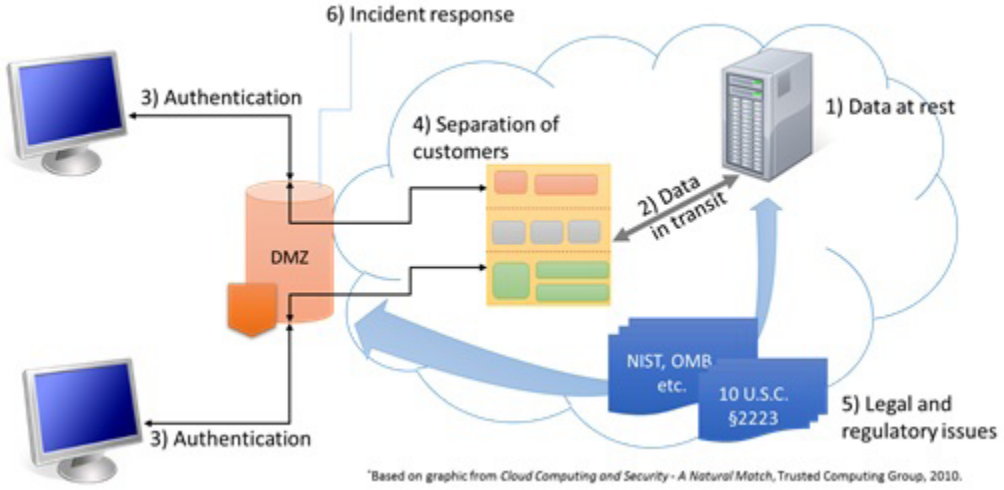

Figure 1: Cloud Security Areas of Concern