INTERACTIVE SESSION MANAGEMENT

How Secure Is the Cloud?

Over the last several years, many companies have altered their IT strategies to shift an increasing share of their applications and data to public-cloud infrastructure and platforms. However, using the public cloud disrupts traditional cybersecurity models that many companies have built up over years. As a result, as companies make use of the public cloud, they need to revise their cybersecurity practices in order to consume public-cloud services in a way that enables them both to protect critical data and to fully exploit the speed and agility that these services provide.

Managing security and privacy for cloud services is similar to managing traditional IT infrastructures. However, the risks may be different because some, but not all, responsibilities shift to the cloud service provider. The category of cloud service (IaaS, PaaS, or SaaS) affects exactly how these responsibilities are shared. For IaaS, the provider typically supplies and is responsible for securing basic IT resources such as machines, storage systems, and networks. The cloud services customer is typically responsible for its operating system, applications, and corporate data placed into the cloud computing environment. This means that most of the responsibility for securing the applications and the corporate data falls on the customer.

Cloud service customers should carefully review their cloud services agreement with their cloud provider to make sure their applications and data hosted in cloud services are secured in accordance with their security and compliance policies. But that's not all. Although many organizations know how to manage security for their own data center—they're unsure of exactly what they need to do when they shift computing work to the cloud. They need new tool sets and skill sets to manage cloud security from their end to configure and launch cloud instances, manage identity and access controls, update security controls to match configuration changes, and protect workloads and data. There's a misconception among many IT departments that whatever happens in the cloud is not their responsibility. It is essential to update security requirements developed for enterprise data centers to produce requirements suitable for the use of cloud services. Organizations using cloud services often need to apply additional controls at the user, application, and data level.

Cloud service providers have made great strides in tightening security for their areas of responsibility. Amazon's security for its cloud service leaves little to chance. The company keeps careful constraints around its staff, watches what they do every day, and instructs service teams to restrict access to data through tooling and automation. Amazon also rotates security credentials for authentication and verification of identity and changes them frequently—sometimes in a matter of hours.

The biggest threats to cloud data for most companies involve lack of software patching or misconfiguration. Many organizations have been breached because they neglected to apply software patches to newly identified security vulnerabilities when they became available or waited too long to do so. (See the discussion of patch management earlier in this chapter.) Companies have also experienced security breaches because they did not configure aspects of cloud security that were their responsibility. Some users forget to set up AWS bucket password protection. (A bucket is a logical unit of storage in Amazon Web Services [AWS] Simple Storage Solution S3 storage service. Buckets are used to store objects, which consist of data and metadata that describes the data.) Others don't understand basic security features in Amazon such as resource-based access policies (access control lists) or bucket permissions checks, unwittingly exposing data to the public Internet.

Financial publisher Dow Jones & Co. confirmed reports in July 2017 that it may have publicly exposed personal and financial information of 2.2 million customers, including subscribers to *The Wall Street Journal* and *Barron's*. The leak was traced back to a configuration error in a repository in AWS S3 security. Dow Jones had intended to provide semi-public access to select customers over the Internet. However, it wound up granting access to download the data via a URL to "authenticated users," which included anyone who registered (for free) for an AWS account. Accenture, Verizon, Viacom, Tesla, and Uber Technologies are

other high-profile names in the steady stream of companies that have exposed sensitive information via AWS S3 security misconfigurations. Such misconfigurations were often performed by employees who lacked security experience when security configurations should have been handled by skilled IT professionals. Stopping AWS bucket misconfigurations may also require enacting policies that limit the damage caused by careless or untrained employees.

Although customers have their choice of security configurations for the cloud, Amazon has been taking its own steps to prevent misconfigurations. In November 2017, the company updated its AWS dashboard, encasing *public* in bright orange on the AWS S3 console so that cloud customers could easily see the status of access permissions to buckets and their objects. This helps everyone see more easily when an Amazon S3 bucket is open to the public. Amazon also added default encryption to all objects when they are stored in an AWS bucket and access control lists for cross-region replication. Another new tool called Zelkova examines AWS S3 security policies to help users identify which one is more permissive than the others. Amazon Macie is a managed service that uses machine learning to detect personally identifiable information and intellectual property, and has been available for S3 since August 2017.

Sources: Kathleen Richards, "New Cloud Threats as Attackers Embrace the Power of the Cloud," SearchCloudSecurity.com, April 3, 2018; "AWS S3 Security Falls Short at High-profile Companies," SearchCloudSecurity.com, April 2018; "Making a Secure Transition to the Public Cloud," *McKinsey & Company,* January 2018; and "Security for Cloud Computing: Ten Steps to Ensure Success," Cloud Standards Customer Council, December 2017.