22 SEP 2017 OPINION

Big Questions to Ask About Security in the Cloud

info security
STRATEGY | INSIGHT | TECHNOLOGY

Published in www.infosecurity-magazine.com/opinions/big-questions-ask-security-cloud/

Srivats Ramaswami CTO at 42Q
Follow @42qMES

Manufacturers deal with sensitive data every day: test and quality data, warranty information, device history records, and especially the engineering specifications for a product are highly confidential. Trusting that data to a cloud-based application or cloud services provider is a big step, and manufacturers need to educate themselves about the security risks and advantages of cloud-based software.

Consider the four questions below as a guide to use when discussing application infrastructure and operations with cloud providers.

How do I know that my data can't be accessed by other customers?
There are many ways to ask this question: Do you mix my data with other companies' data? Can other people see my data? What's your database structure for each customer? The answer to each of these is data separation. The system architecture should ensure separation of customer data by customer organization, usually by individual factory or site. This allows even customer administrative tasks such as assigning roles to be limited in scope.

While many applications are multi-tenant (meaning the application is shared across multiple customers), transactional data should still be separated by customer factory, meaning there is no commingling of customer data. In other words, your data will be separated from every other customer, giving the highest level of data separation.

What do you do to prevent the data from being hacked and stolen?
"Hacking" or stealing data is the number one security concern of most people considering a cloud solution. Note, however, that some common misunderstandings often drive this concern.

According to the latest Data Breach Investigations Report from Verizon, approximately 50% of all security incidents are caused by people inside an organization. Good user management and password security policies are the best way to prevent these types of attacks. This is the underlying purpose of application password protection, as described above.

For preventing external hacks and data theft, the system must be architected to prevent as many types of attacks as possible (see above). Also, application providers must use internal personnel and external consultants to run frequent penetration testing. These tests look for common paths that attackers use to gain access to systems through the internet. The tests help ensure there are no doors left open for hackers. Be sure to ask about penetration testing, including both the frequency and the methodologies used.

Are there any security certifications from third parties that I should know about?
Rather than trusting the word of a technology provider, many companies have come to rely on third party certifications for judging the security architecture and processes used by cloud providers. One of the most important of these is SOC 2 certification.

Developed by the AICPA, SOC 2 is specifically designed for service providers storing customer data in the cloud. That means SOC 2 applies to nearly every cloud or "software as a service" company.

So what does SOC 2 require, exactly? It's considered a technical audit, but it goes beyond that: SOC 2 requires companies to establish and follow strict information security policies and procedures, encompassing the security, availability, processing, integrity and confidentiality of customer data. SOC 2 ensures that a company's information security measures are in line with the unique parameters of today's cloud requirements. As companies increasingly leverage the cloud to store customer data, SOC 2 compliance is becoming a necessity for a wide variety of organizations. Consider making it one of your requirements for any cloud provider.

How does cloud security compare to on-premise security?
This is a question to ask internally as well as externally. There is a common misperception that a set of servers running on-premise at a corporate office is more secure than a cloud-based application. Owning the hardware and software often gives a false sense of security; most on-premise systems fall far short of the security that the best cloud providers have deployed.

For example, the cloud storage system utilized by my company was designed for 99.999999999% durability and up to 99.99% availability of objects over a given year. That design and those numbers are virtually impossible to duplicate with an on premise solution. In addition, the comprehensive access control described above is nearly impossible to duplicate on-premise. To deploy tools like these in an on-premise environment would require not only large investments in infrastructure, but large teams to manage them too.

Ask yourself: how big is your security team? How much is your budget for security around your manufacturing data? Then remember, the best application providers and data centers have large, dedicated security teams who have implemented automated threat monitoring systems that operate 24x7. In the end, the best cloud software companies have dedicated more time, resources and budget to securing our systems than most organizations are able to provide themselves.