WEI INSIGHTS TECH BRIEF

SIX OVERLOOKED TACTICS TO IMPROVE CLOUD SECURITY

Not long ago, many organizations were reluctant to adopt cloud technologies or Anything-as-a-Service in large part because of concerns about security and loss of data control. After all, the traditional approach to network security is heavily focused on protecting the network perimeter. How do you do that when the Internet is being used to interact with applications, services, and data? It's no surprise that enterprises were a bit unsettled with the idea of sharing the responsibility of security and privacy with cloud providers.

Enterprises remain concerned. Only 15 percent of IT decision makers are confident there are no risks with their cloud provider, according to Recent IDG research commissioned by Worldcom Exchange, Inc. (WEI). The research also revealed that either data privacy or data loss is the top cloud security concern for nearly 70 percent, while nearly 20 percent said their top cloud security concern was employee access to the cloud.

You might assume based on those gloomy statistics that cloud adoption rates would be low. Not so. The cloud technology market is growing globally by about $6 billion per year by some estimates. Enterprises can bolster cloud security with a few best practices that are often overlooked.

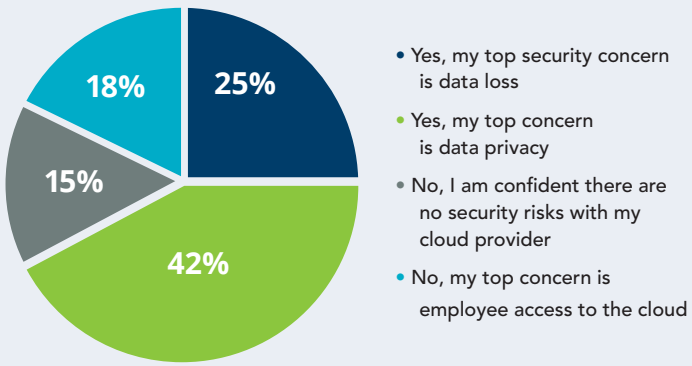
1. ENSURE TIMELY UPDATES.

Hackers use the same attack methods against cloud technologies and on-premises technologies. In either case, attack methods include exploited application vulnerabilities, Advanced Persistent Threats, malware such as ransomware, insider attacks, social engineering, and easily guessed passwords. Therefore, the same precautions that protect an enterprise network will be effective in protecting cloud technology. For instance, end user operating systems and applications should be updated, especially the web browser used to access cloud applications. In addition, cloud technologies should comply with enterprise policies for password expiration and complexity.

2. DEVELOP A FORMAL CLOUD SECURITY STRATEGY.

Some industry analysts report only about a third of enterprises have a documented cloud security strategy. Strategy topics could include use cases for public, private, and hybrid cloud delivery options; overarching enterprise standards for Service Level Agreements; appropriate use of multi-tenant environments (environments shared with other customers); any encryption requirements for data in transit and at rest; guidelines for integrating with in-house technology; data transit across geographic jurisdictions, and compliance with applicable laws and regulations in those jurisdictions.

Do you have security concerns about your cloud provider?



IDG TechPulse poll of 102 ITDMs | February 23, 2016 | Commissioned by Worldcom Exchange, Inc.

WEI

3. REVIEW THE SECURITY OF CLOUD PROVIDERS.

Whether for an existing or new cloud provider, you should understand the provider's security posture. Ask your cloud provider for the following documents:

- Service Level Agreements and other contractual documents which address any uptime or support commitments, calculation of refunds for any uptime guarantees, calculation of breach liability, monthly reporting on security events and responses, enterprise ability to monitor cloud systems, enterprise ability to conduct security assessments, enterprise access to event logs, geographic jurisdictions of all involved data centers, and data storage upon contract termination
- Architecture documents
- Documents that explain cyber liability and Errors & Omissions insurance coverage
- Plans and policies for disaster recovery, incident response, issue escalation, business continuity, notification of breaches (for the enterprise or other customers), and ongoing employee and contractor screening
- Documentation that describes security technology that supports uptime such as backups, monitoring, anti-malware, anti-intrusion, redundancy, automatic failover, encryption, and handling of cryptographic keys
- Information about physical access control, logical access control, and authentication standards
- SOC 1 (SAS 70) or another review or certification of controls
- Financial statement to ensure the provider's viability
- Customer references
- History of security incidents or breaches
- History of lawsuits or legal action
- Any internal or third-party security assessment reports

4. ESTABLISH A PROCESS FOR USERS TO REQUEST NEW CLOUD SERVICES AND SOFTWARE.

Shadow IT is the term that describes technology that is used within an enterprise without proper approval. For the 2015 Cloud Adoption Practices and Priorities Survey Report, the Cloud Security Alliance defined Shadow IT as "technology spending and implementation that occurs outside the IT department, including cloud apps adopted by individual employees, teams, and business units." Ninety-two percent of organizations surveyed said they did not know the scope of Shadow IT, the report noted. This includes 20 percent of all organizations that in effect said that they didn't know and also didn't care.

Some enterprises have approached the problem by blocking popular cloud services, the report said, but this practice sometimes has negative security consequences. Blocking popular tools tends to drive workers toward less popular tools that haven't been subjected to the exhaustive security rigors of large enterprises, and these tools are typically less secure.

5. STEP UP MONITORING, ESPECIALLY FOR MACHINE-TO-MACHINE COMMUNICATION.

Monitoring solutions typically do a good job of monitoring CPU, memory, storage, machine-to-user communication (North-South traffic), and perimeter traffic. However, most organizations have no visibility into traffic between applications, systems, and virtual machines in data centers and cloud environments, according to a 2015 SANS Institute white paper on the state of data center and cloud security. Effective monitoring of machine-to-machine communication (East-West traffic) could provide an early indication of an attacker inside the network who is attempting to move laterally to other network segments. These attacks could include slow-moving, multi-step Advance Persistent Threats or enterprise ransomware, a threat that is quickly emerging in 2016. Tools used to monitor East-West traffic include intrusion detection and prevention systems, malware

detection tools, and access control lists on intermediate routers and switches, the SANS paper noted. Monitoring should occur as close to the workload as possible, such as at individual systems and virtual machines. The challenge is to block malicious traffic while not disrupting legitimate operations. Because many organizations have not identified legitimate East-West traffic, an initial inventory exercise might be needed.

6. REVIEW CLOUD INSURANCE COVERAGE.

Issues related to the division of responsibility between an enterprise and its cloud provider quickly come into focus when considering a security breach. With security responsibilities shared, who pays when cloud security fails?

The formula used to calculate the provider's share of liability is specified in the cloud contract and in some cases can be negotiated like any other contract term. In addition, some enterprises require cloud providers to pay either the enterprise's deductible or costs that exceed coverage limits in the event of a claim. Enterprises should review the provider's cyber liability coverage, especially because some policies do not cover lost revenues or increased expenses due to cloud outages. Enterprises should check for Contingent Business Interruption language.

In addition, enterprise officers and members of Boards of Directors should be insured against shareholder class action law suits via Directors and Officers Insurance. Executives with Target, Wyndham Worldwide, Sony Pictures Entertainment, Home Depot, and other enterprises have faced one or more shareholder suits in the wake of large-scale breaches. Shareholders initiate these suits on behalf of a corporation, alleging the corporation was harmed when executives failed to provide effective security oversight.

WHERE TO START

After reviewing these key considerations for improving cloud security, you might be asking -- where is the most logical place to start? The recommended next step is to get a professional security assessment, but tread carefully. Partner with a company whose assessment goes above and beyond identifying where the potential security risks are; look for a company that takes the time to understand your business and how your employees interact with cloud applications. The right company will help you implement the overlooked cloud security tactics mentioned above, and help you develop a bulletproof cloud security strategy aligned with the right security solutions for your IT environment and business goals.

TALK TO WEI TODAY

Learn about our free Security and Threat Prevention Assessment which identifies vulnerabilities in your network and provides personalized recommendations for improved security.

ABOUT WEI

WEI is an innovative, full service, customer centric IT solutions provider.

Why WEI? Because we care. *Because we go further.*

At WEI, we're passionate about solving your technology problems and helping you drive your desired business outcomes. We believe in challenging the status quo and thinking differently. There are a lot of companies that can take today's technology and create a great IT solution for you. But we do more. We go further. And we have the customer, vendor and industry awards to prove it. WEI is a premier technology partner, who always puts our customers first while providing the most innovative solutions for over 25 years.

WEI Dedication meets innovation.
info@wei.com
www.wei.com
43 Northwestern Drive | Salem, NH 03079
800.296.7837