AT&T Cybersecurity Blog

Securing your cloud networks: Strategies for a resilient infrastructure

August 17, 2023 | Vina Nguyen

The content of this post is solely the responsibility of the author. AT&T does not adopt or endorse any of the views, positions, or information provided by the author in this article.

What exactly is resilience? According to the U.S. National Institute of Standards and Technology, the goal of cyber resilience is to "enable mission or business objectives that depend on cyber resources to be achieved in a contested cyber environment." In other words, when you're at odds with cybercriminals and nation-state actors, can you still get your job done? If not, how quickly can you get back up and running? In this article, we outline steps to ensure that if your cloud networks fail, your business won't fail along with them.

Take stock of what you can't (and can) live without

Being resilient during and post-cyber-attack means being able to continue business operations either leanly or back to full throttle soon after. While resources are being pooled to respond and recover from an incident, what data must be protected and what operations must go on?

Data that must be protected include those defined by regulation (e.g., personal identifiable information), intellectual property, and financial data. Data itself must be protected in multiple forms: at rest, in transit, and in use. The type of business you're in may already dictate what's essential; critical infrastructure sectors with essential operations include telecommunications, healthcare, food, and energy. Anything that your business relies on to survive and sustain should be treated as highest priority for security.

Ensure required availability from your cloud provider

An essential part of resilience is the ability to stay online despite what happens. Part of the cloud provider's responsibility is to keep resources online, performing at the agreed level of service. Depending on the needs of your business, you will require certain levels of service to maintain operations.

Your cloud provider promises availability of resources in a service-level agreement (SLA), a legal document between the two parties. Uptime, the measure of availability, ranges from 99.9% to 99% in the top tiers of publicly available clouds from Amazon and Microsoft. A difference of 0.9% may not seem like much, but that translates from roughly 9 hours of downtime to over 3.5 days annually—which might be unacceptable for some types of businesses.

Store backups—even better, automate

As ransomware proliferates, enterprises need to protect themselves against attackers who block access to critical data or threaten to expose it to the world. One of the most fundamental ways to continue business operations during such an incident is to rely on backups of critical data. After you've identified which data is necessary for business operations and legal compliance, it's time to have a backup plan.

While your cloud service provider provides options for backup, spreading the function across more than one vendor will reduce your risk—assuming they're also secure. As Betsy Doughty, Vice President of Corporate Marketing of Spectra Logic says, "it's smart to adhere to the 3-2-1-1 rule: Make three copies of data, on two different mediums, with one offsite and online, and one offsite and offline." Automated snapshots and data backup can run in the background, preparing you in the event of a worst-case scenario.

Expose and secure your blind spots

A recent report from the U.S. Securities and Exchange Commission observes that resilience strategies include "mapping the systems and process that support business services, including those which the organization may not have direct control." Cloud networks certainly apply here, as with any outsourced services, you relinquish some control.

Relinquishing control does not have to mean lack of visibility. To gain visibility into what data is being transferred and how people are using cloud applications, consider the services of cloud access service brokers (CASBs), who sit between a cloud user and cloud provider. CASBs can improve your resilience providing detail into your cloud network traffic, enabling assessment for both prevention of attack and impact on business operations in the event of an incident. They also enforce security policies in place such as authentication and encryption.

Test your preparedness periodically

After all the hard work of putting components and plans into place, it's time to put things to the test. Incident response tests can range from the theoretical to a simulated real-world attack. As processes and people change, performing these tests periodically will ensure you have an updated assessment of preparedness. You could run more cost-effective paper tests more frequently to catch obvious gaps and invest in realistic simulations at a longer interval. Spending the resources to verify and test your infrastructure will pay off when an attack happens and the public spotlight is on you.

Towards a resilient cloud

Being able to withstand a cyber-attack or quickly bring operations back online can be key to the success of a business. While some responsibility lies in the cloud provider to execute on their redundancy and contingency plans per the SLA, some of it also lies in you. By knowing what's important, securing your vulnerabilities, and having a tested process in place, you are well on your way to a secure and resilient cloud network.

Share this with others

Tags: shared security model, resilience, casb, cloud computing, service level agreement, sla

---