Hey! What’s New? 2024-85

Data Security in the Age of Cloud Computing

A recent article in the *Data Administration Newsletter*, written by Ainsley Lawrence, notes that, with companies transitioning their assets and storing their data on the cloud come new and possibly critical security risks. “Data breaches, unauthorized access to company resources, privacy, and out-and-out information losses are all among the threats facing companies that use cloud computing today. Understanding how to safeguard your cloud computing network against these threats is vital to using the technologies effectively, avoiding reputational damage, and aligning yourself with regulatory standards.”

This article, therefore, examines the challenges inherent to cloud computing and offers for using this technology to its fullest extent.

It starts by addressing the elephant in the room: hackers. “Cybercrime has been on the rise for years now and is projected to cost the world $15.63 trillion by 2029. For cybercriminals looking for a quick score, organizations that use cloud computing and store sensitive data on their network are at the top of the priority list. Without the proper security measures in place, a cybercriminal can easily get into your company systems and wreak all kinds of havoc, and you might not know about it until it’s too late.”

Lawrence says that most leaders know that data breaches are a risk, but they might not know how to protect company data in an entirely new, 100% digital network environment. “While common cybersecurity best practices like network patching and antivirus protection will help control physical access points, how do you protect access to a service that you don’t own and can’t fortify in a traditional manner?”

She then suggests some cloud computing network protection best practices:

- **Controlling access:** Cloud computing solutions typically come with controls that allow you to control access to data on a granular level. “Identity and access management tools assign permissions to users on an individual basis, allowing them to access select groups of sensitive information and rebuffing them when they attempt to access blocked-off data. Authentication measures such as two-factor authentication and SSO/SAML authentication provide extra layers of protection.”
- **Encryption:** Encryption is a last line of defense, but a vital one. “Encrypting data at rest shuts down cyber criminals who manage to break into your systems, rendering your sensitive data utterly illegible to unauthorized users.”
- **Backups:** Backing up your data regularly will allow you to quickly recover in the event of a catastrophe, such as data corruption or data loss. “Performing regular backups is a vital insurance policy, as it will empower you to restore lost information on a dime and treat incidents that would wreck the unprepared as minor hiccups.”
- **Penetration and disaster recovery testing:** Regularly testing network penetration and your disaster recovery readiness helps identify vulnerabilities and hiccups in your recovery process. “With the information from these tests, you can then add additional controls to

> cover holes in your network security and streamline your recovery process to ensure smooth sailing.”

Lawrence also suggests leveraging newer technologies, such as AI and machine learning, to provide extra layers of security. “Machine learning algorithms can scan your network activity, identify anomalies, and report on them at near-lightning speed, unlocking a rapid response from your cybersecurity team. AI can also supplement authentication controls by contrasting user actions with a profile of historical behavior, flagging potentially risky actions and shutting off access rapidly.

But even with these measures in place, warns Lawrence, “there’s still a degree of risk involved when using cloud computing. Risks that an employee will misuse their access, store data out of accordance with regulatory best practices, or accidentally open a window for cybercriminals to sneak in through. Managing these risks falls on you, as the leader, to create an infrastructure that makes your employees aware of and accountable to best practices.”

You’ll want to set up a clear feedback loop for when a threat is detected. “Employees should know how to report a threat and should be encouraged to do so as quickly as possible to allow for a rapid organizational response. Encouraging collaboration and active communication among team members as well as having more eyes on each data set will make it easier for your employees to correctly identify emergent threats.”

For more, see Data Security in the Age of Cloud Computing – TDAN.com.