Cloud Security 101

Why are businesses switching to the Cloud?

More and more businesses are switching to the Cloud to store their data and rightly so. The Cloud offers numerous benefits over the traditional, physical on site server. For example,

- **Anytime, anywhere access to your data:** Information in the Cloud can be accessed from anywhere using an internet connection, unlike in the case of traditional servers, where you need a physical connection to the servers
- **Significant cost savings:** You cut hardware costs, because you are not investing in physical hardware.
- **Shared storage means more cost savings:** The Cloud lets you share space with others while maintaining a secure environment in general. It follows a 'pay-as-you-use' approach to data storage allowing you to enjoy cost savings based on your data storage needs, unlike the traditional options where you had to pay for and purchase a whole new server if your data storage needs exceeded the existing capacity.
- **SaaS compatibility and support:** The Cloud allows the use of Software-as-a-Service since the software can be hosted in the Cloud
- **Scalability:** The Cloud lets you scale up and down as your business needs change
- **24/7 monitoring, support, and greater access reliability:** When your data is in the Cloud, the Cloud service provider is responsible for keeping it safe and ensuring it is securely accessible at all times. They monitor the cloud's performance and in the event of any performance issues, they provide immediate tech support to resolve the problem

Is the Cloud really risk-free

While all the above-mentioned factors make the Cloud a very attractive choice, especially for SMBs who don't want to be burdened with higher in-house IT costs, putting your data in the Cloud is not risk-free. Just as storing data on physical servers has its security threats, the Cloud presents certain security concerns as well. These include

- **Data breach:** A data breach is when your data is accessed by someone who is not authorized to do so.
- **Data loss:** A data loss is a situation where your data in the Cloud is destroyed due to certain circumstances such as technological failure or neglect during any stage of data processing or storage.
- **Account hijacking:** Like traditional servers, data in the Cloud could be stolen through account hijacking as well. In fact, Cloud account hijacking is predominantly deployed in cybercrimes that require identity thefts and wrongful impersonation
- **Service traffic hijacking:** In a service traffic hijacking, your attacker first gains access to your credentials, uses it to understand the online activities that happen in your domain and then uses the information to mislead your users or domain visitors to malicious sites.
- **Insecure application program interfaces (APIs):** Sometimes, Cloud APIs, when opened up to third parties, can be a huge security threat. If the API keys are not properly secured, it can serve as an entry point for cybercriminals and malicious elements.
- **Poor choice of Cloud storage providers:** A security lapse from the Cloud storage provider's end is a huge security concern for businesses. It is very important to choose a trusted and experienced Cloud service provider who knows what they are doing.

Apart from the above, there are some common threats that apply to both the Cloud and traditional data storage environments such as a DDoS attack, or a malware attack where your data in the Cloud becomes susceptible because it is being shared with others and at other places.

3 key steps to take to protect your data from the security threats presented above

- **Secure access:** The first step would be to secure access to your data in the Cloud. So, how do you go about it? safeguard your login credentials–your User IDs and passwords–from prying eyes strong password policies that are practiced across the board and educate your employees about good password hygiene. Also, do you have employees using their own devices to access their work-related applications and documents? Do you have staff working from home? Then, you also need to formulate strong BYOD (Bring-your-own-device) policies, so these devices don't end up as the entry point to cybercriminals.

- **Educate your employees:** What's the first thing that pops into your head when someone talks about cybercrime? You probably picture some unknown person, a tech-whiz sitting behind a computer in a dark room, trying to steal your data. But, surprising as it may seem, the first and probably the biggest threat to your data and IT security in general, comes from your employees! Malicious employees may do you harm on purpose by stealing or destroying your data, but oftentimes, employees unwittingly become accomplices to cybercrime. Some examples include-
    - Forwarding an email with an attachment that contains a virus
    - Clicking on a phishing link unknowingly and entering sensitive information therein
    - Compromising on security when they share passwords or connect to an unsecured or open WiFi at public places such as the mall or the airport

A lot of time cybersecurity breaches happen when employees function with a view to "get things done faster", but, without realizing how disastrous the implications of such actions can be.

- **Choosing the right Cloud service provider:** If you are putting your data in the cloud, you need to make sure that it is in safe hands. As such, it is your Cloud service provider's responsibility to ensure your data is secure and accessible, always. But, are they doing all that is needed to ensure this happens? It is very important to choose a trustworthy Cloud service provider because you are essentially handing over all your data to them. So, apart from strengthening your defenses, you need to check how well-prepared they are to avert the threats posed by cybercriminals.

Cloud security mechanisms

- **Cloud firewalls:** Much like the firewalls you deploy for your local IT network, Cloud firewalls work to prevent unauthorized Cloud network access.
- **Penetration testing:** Penetration testing is a sort of a Cloud security check where IT experts try hacking into the Cloud network to figure out if there are any security lapses or vulnerabilities that could serve cybercriminals.
- **Obfuscation:** In obfuscation, the data or program code is obscured on purpose such that the system delivers unclear code to anyone other than the original programmer, thus mitigating any malicious activity.
- **Tokenization:** Tokenization is the process of replacing sensitive data with unique identification symbols that retain all the essential information about the data without compromising its security.[1]
- **Virtual Private Networks (VPN):** Another, more commonly used mechanism is the VPN. VPN creates a safe passage for data over the Cloud through end-to-end encryption methodology.

Investing in a good Cloud security system is a must, but, in the end, you also need to remember that Cloud security is not only about antivirus software, firewalls, and other anti-malware tools. Complete Cloud security is a blend of all these plus internal policies, best practices, and regulations related to IT security, and of course, the MSP you choose to be your Cloud security provider plays a key role in all this. You need to pick the right MSP and work closely with them to implement a Cloud security solution that works for you.

For more information please contact,
Dale Roberts | Principal | Centarus
Phone: (415) 671-7560 | Email: dale@centarus.co