Cloud Security Challenges

The cloud can seem abstract, and just that: cloudy. Customers want to know what policies and practices are in place to ensure security. On the other hand, cloud service providers need to commit to a high level of transparency, to assure customers that their data is secure. Luckily for customers, cloud infrastructure providers are competing with each other, meaning that they all put customers' trust first.

Why use the cloud in the first place?

There are major advantages when using the cloud for some part of the operational IT infrastructure, as well as using the cloud to provide services to customers:

1. The size of your infrastructure can be adapted dynamically. This flexibility is great for fast-growing companies as well as those unsure of future demand: and really, who isn't?
2. Online-services in the cloud are more cost-effective than using proprietary IT infrastructure. That's really why cloud services started out in the first place: shared infrastructure means less cost per user.

Complex security needs

Trends in today's economy impact how businesses use the cloud. For example, globalization, public private partnerships, quickly changing demand levels: all impact the cloud service providers. Public sector companies have different security needs than government agencies. Government agencies in one country have different security policies than in another country. As soon as customers in one country use cloud servers located in another country, international law comes into play. Dynamically adapting server capacity to changing needs implies another level of complexity in cloud security.

The hosting company needs to have a solid framework of security policy and technology.

Good questions to ask of your online services provider in the cloud

So how do you make sure that your cloud service provider considers all the security challenges and has proven policies and processes in place to protect you? Ask them questions, and see how they answer these: are the answers satisfactory, extensive and prove that they have processes in place? Some good questions to ask:

- Do they have dedicated security staff?
- What kind of security regulations do they follow?
- Do they comply with international requirements?
- Where are their data centers?

Approaches to Cloud Security

It does not make sense to put pennies in a high-security bank vault. The cost of security far outweighs the value of the asset. Similarly, security requirements need to consider the value of the assets protected by the policy and controls.

Typically, a cloud security policy covers the requirements phase, the modeling of threats and the analysis of the attack surface, a full test of the controls, and finally, training and education.

Elements of a security framework

A comprehensive security framework consists of:

- A proprietary security policy covering standards, baselines and standard operating procedures
- External requirements: regulatory and industry obligations
- Control activities with designated owners to ensure that requirements and policy are followed
- Audits make sure that the control activities are carried out, requirements met, and security policy is followed.

Compliance with government and industry security requirements

In addition to company proprietary security programs and policies, governments around the world impose stringent security requirements on cloud service providers.

Examples of well-recognized security certifications from government and industry are: ISO/IEC 27001:2005 certification, SSAE 16/ISAE 3402 SOC 1 Type I and Type II and AT Section 101 SOC 2 and 3 Type I and Type II attestations, as well as FISMA Certification and Accreditation.

Ultimately, it is the customer's privilege to choose the service provider and the level of security necessary for their use.

So how do you evaluate cloud security?

Ask how the security policies and frameworks are structured. As soon as payments are being processed, security goes up to a whole other level.

One security best practice across the industry is Defense-in-depth. It involves controls at multiple layers and employing protection mechanisms, developing risk mitigation strategies, and responding effectively to attacks when they occur. A tiered system of security means that more sensitive information is protected with more complex measures, and results in improved capacity to prevent breaches or to lessen the impact of a security incident.

Defense-in-depth strategy means that if one area should fail, protections are in place in other areas to compensate. The different areas are

- Physical access control,

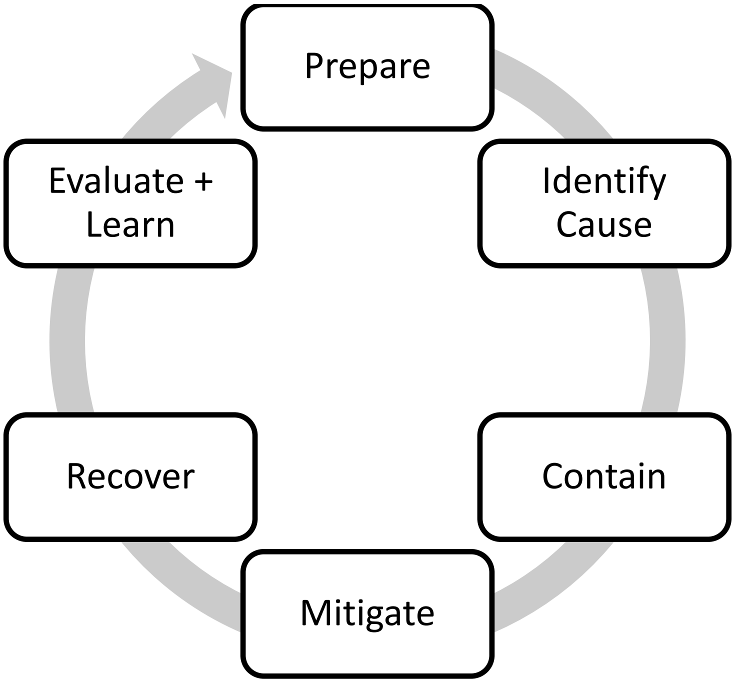
- Encryption of any data transfer,
- Up-to-date malware protection,
- Appropriate safeguards for all applications,
- The ability to lock down the host servers.

Response to Cloud Security Incidents

Your worst nightmare: a security breach in the cloud. Are the anti-tech, anti-progress people right, after all?

What you don’t even dare to imagine, cloud service providers do every day: they imagine the worst case scenarios and put solid security measures in place preventing them from becoming reality. A dedicated team operating 24/7 responds to any potential issues as they arise.

An incident response process is really an on-going process, even without incidents occurring: always researching and being up to date on the most recent threats. When the incident occurs, the response team will identify the cause, so they can quickly contain the breach. Next, they put in place mitigating measures to prevent future occurrence of this breach. Services are recovered as quickly as possible, and this step also includes extensive testing of the mitigation put in place. The last step in this on-going process is possibly the most important: the team evaluates what happened and notes lessons learned.


Prepare
Identify Cause
Contain
Mitigate
Recover
Evaluate + Learn