OWASP Cloud Top 10

Top 10 Cloud Security Risks

DRAFT

Ludovic Petit

SFR

Chapter Leader OWASP France

OWASP Global Connections Committee

Ludovic.Petit@owasp.org
About me

- Group Fraud & Information Security Adviser at SFR
- Member OWASP Global Connections Committee
- Translator of the OWASP Top Ten
- Chapter Leader OWASP France
- Contributions & Reviews
  - OWASP Secure Coding Practices - Quick Reference Guide
  - OWASP Mobile Security Project
  - OWASP Cloud Top10 Project
Agenda

- Motivation
- Cloud Top 10 Security Risks
- Summary & Conclusion
- Q&A
Motivation

Develop and maintain Top 10 Risks with Cloud
Serve as a Quick List of Top Risks with Cloud adoption
Provide Guidelines on Mitigating the Risks
Building Trust in the Cloud
Data Protection in Large Scale Cross-Organizational Systems
Cloud Top 10 Risks

- R1. Accountability & Data Risk
- R2. User Identity Federation
- R3. Legal & Regulatory Compliance
- R4. Business Continuity & Resiliency
- R5. User Privacy & Secondary Usage of Data
- R6. Service & Data Integration
- R7. Multi-tenancy & Physical Security
- R8. Incidence Analysis & Forensics
- R9. Infrastructure Security
- R10. Non-production Environment Exposure
R1. Accountability & Data Risk

A traditional data center of an organization is under complete control of that organization. The organization logically and physically protects the data it owns.

An organization that chooses to use a public cloud for hosting its business service loses control of its data. This poses critical security risks that the organization needs to carefully consider and mitigate.

One must ensure about the guarantee of recovering Data:

- Once the data entrusted to a third operator, what are the guarantees that you will recover your information?

- What about the backups performed by the operator of Cloud?
It is very important for the enterprises to keep control over user identities as they move services and applications to the different cloud providers.

Rather than letting Cloud providers create multiple islands of identities that become too complex to manage down the line.

Users should be uniquely identifiable with a federated authentication (e.g. SAML) that works across cloud providers.

User experience is enhanced when he/she does not manage multiple userids and credentials. This allows for back-end data integrations between cloud providers.
R3. Legal & Regulatory Compliance

It is complex to demonstrate Regulatory compliance.

Data that is perceived to be secure in one country may not be perceived secure in another due to different regulatory laws across countries or regions.

For instance, European Union has very strict privacy laws and hence data stored in US may not comply with those EU laws.
R4. Business Continuity & Resilency

Business Continuity is an activity an IT organization performs to ensure that the business can be conducted in a disaster situation.

In case of an organization that uses cloud, the responsibility of business continuity gets delegated to the cloud provider.

This creates a risk to the organization of not having appropriate business continuity.

For Service Continuity and QoS, one have to ensure about

- the contractual solutions proposed by the Operator of Cloud,
- the Service Level Agreement as well
R5. User Privacy & Secondary Usage of Data

User's personal data gets stored in the cloud as users start using social web sites. Most of the social sites are vague about how they will handle users personal data.

Additionally most of the social sites go with the default share all (least restrictive) setup for the user. E.g. LinkedIn, Twitter, Facebook it is very easy to deduct personal details of the users.

You need to ensure with your Cloud providers what data can or cannot be used by them for secondary purposes.

It includes data that can be mined directly from user data by providers or indirectly based on user behavior (clicks, incoming outgoing URLs, etc.).

Many social application providers mine user data for secondary usage e.g. directed advertising. No wonder when many of us use their personal gmail/hotmail or yahoo account to tell a friend your vacation plans and immediately you start seeing advertisements on hotels/flight near your destination.
Organizations must be sure that their proprietary data is adequately protected as it is transferred between the end user and the cloud data center.

The interception of data in transit should be of concern to every organization, the risk is much greater for organizations utilizing a Cloud computing model, where data is transmitted over the Internet. Unsecured data is susceptible to interception and compromise during transmission.
R7. Multi-tenancy & Physical Security

Multi-tenancy in Cloud means sharing of resources and services among multiple clients (CPU, networking, storage/databases, application stack).

It increases dependence on logical segregation and other controls to ensure that one tenant deliberately or inadvertently can not interfere with the security (confidentiality, integrity, availability) of the other tenants.
In the event of a security incident, applications and services hosted at a Cloud provider are difficult to investigate as logging may be distributed across multiple hosts and data centers which could be located in various countries and hence governed by different laws.

Along with log files, data belonging to multiple customers may be co-located on the same hardware storage devices and hence a concern for law enforcing agencies for forensic recovery.
R9. Infrastructure Security

All infrastructure must be hardened and configured securely, and the hardening/configuration baselines should be based on Industry Best Practices.

Applications, Systems and Networks must be architected and configured with tiering and security zones. Access must be configured to only allow required network and application protocols.

Administrative access must be role-based, and granted on a need-to-know basis. Regular risk assessments must be done, preferably by an independent party.

Policy and process must be in place for patching/security updates, and can based on risk/threat assessments of new security issues.

Although the fine details of the items above must be regarded as highly sensitive information, it is reasonable to expect a customer to want to see at least the high-level details.

Provider must be willing to provide this.
An IT organization that develops software applications internally employs a set of non-production environments for design, development, and test activities. Non-production environments are generally not secured to the same extent as the production environment. If an organization uses a Cloud provider for such non-production environment, then there is a high risk of unauthorized access, information modification, and information theft.
Cloud computing is a new way of delivering computing resources, not a new technology.

Computing services (ranging from data storage and processing to software, such as email handling) are available instantly, commitment-free and on-demand.

This checklist should provide a means for customers to

- Assess the risk of adopting Cloud Services
- Compare different Cloud provider offerings
- Obtain assurance from selected Cloud providers
- Reduce the assurance burden on Cloud providers
Want to contribute or provide feedback?

Ludovic.Petit@owasp.org

The OWASP Cloud Top 10 Project

https://www.owasp.org/index.php/Projects/OWASP_Cloud_%E2%80%90_10_Project