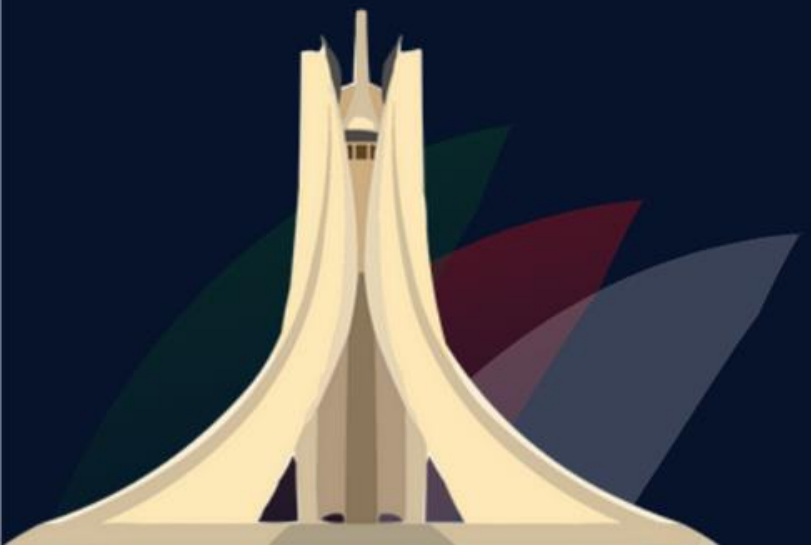
OWASP ALGIERS



Challenges In Cloud Security

20/04/2024

OWASP ALGIERS

SPEAKER

Meriem Maroua MAHDI

Board Secretary @ OWASP Algiers

- Board Member @ OWASP Algiers Chapter
- Cyber Security Specialist
- VAPT Professional, SOC Incident Handler & Solutions Administrator

Agenda

1. Introduction
2. Cloud Deployment Models
3. Cloud Service Models
4. Cloud Security - Shared Responsibility Model
5. The Advantages of Cloud Computing
6. OWASP Top 10 Cloud Security Risks & Mitigations
7. Conclusion

OWASP ALGIERS

Introduction

What Is The Cloud Computing ?

What Is The Cloud Computing ?

- Cloud computing refers to the use of hosted services, such as data storage, servers, databases, networking, and software over the internet.
- The data is stored on physical servers, which are maintained by a cloud service provider. Computer system resources, especially data storage and computing power, are available on-demand, without direct management by the user in cloud computing.

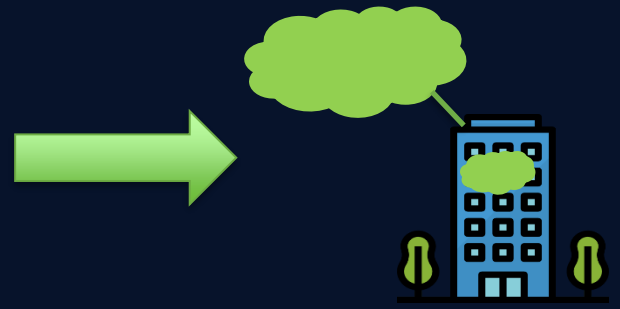
Cloud Deployment Models

Cloud Deployment Models

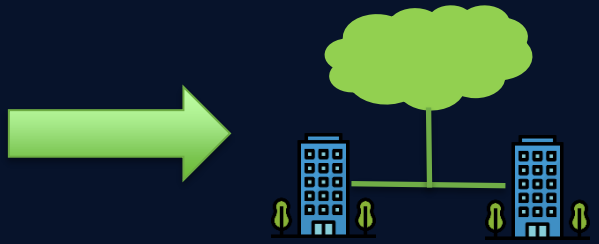
- **Public Cloud**: Manufacturing organization share cloud with general public

- **Private Cloud**: Manufacturing organization has its own cloud private

- **Hybrid Cloud**: Combination of private and public cloud deployment models



- **Community Cloud**: Manufacturing organization shares cloud with other organization with similar interests



Cloud Service Models

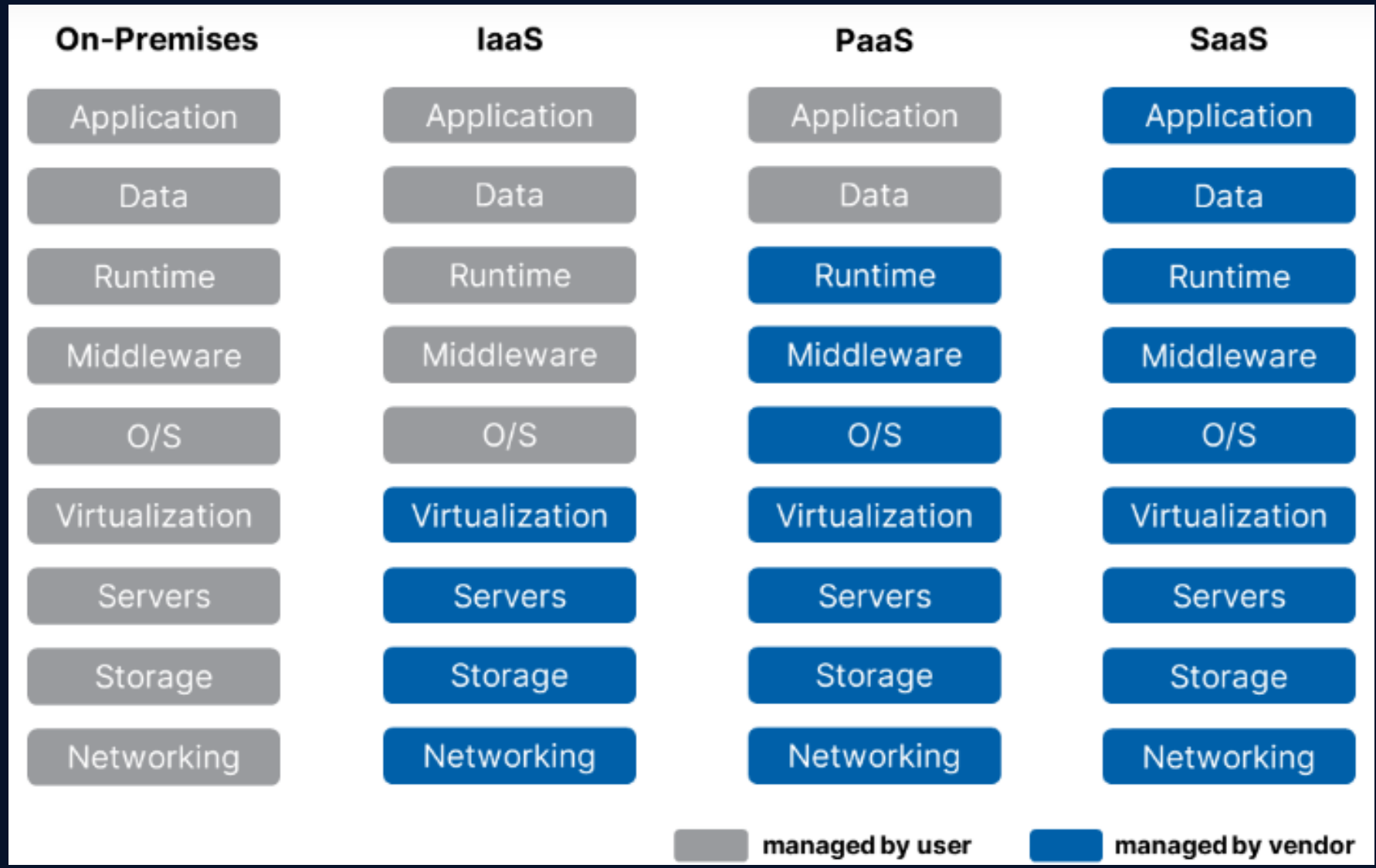
Cloud Service Models

- **Infrastructure As A Service (IaaS)**: on-demand access to cloud-hosted physical and virtual servers, storage and networking—the backend IT infrastructure for running applications and workloads in the cloud.

- **Platform As A Service (PaaS)**: on-demand access to a complete, ready-to-use, cloud-hosted platform for developing, running, maintaining and managing applications.

- **Software As A Service (SaaS):** on-demand access to ready-to-use, cloud-hosted application software.

Cloud Security - Shared Responsibility Model



The Advantages Of Cloud Computing

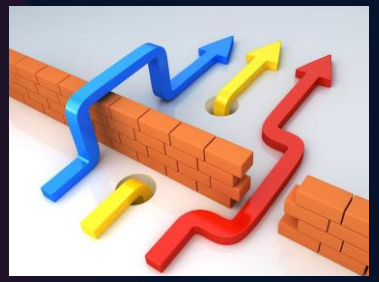
The Advantages Of Cloud Computing

√ “Pay as you Go”

√ Scalability

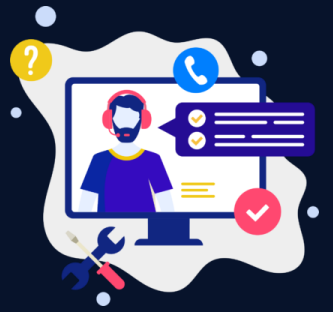
√ Efficiency and Agility

√ Flexibility



√ Security and Reliability

√ Support



OWASP Top 10
Cloud Security Risks & Mitigations

1. Accountability & Data Risk
2. User Identity Federation
3. Legal & Regulatory Compliance
4. Business Continuity & Resiliency
5. User Privacy & Secondary Usage of Data
6. Service & Data Integration
7. Multi-tenancy & Physical Security
8. Incidence Analysis & Forensics
9. Infrastructure Security
10. Non-production Environment Exposure

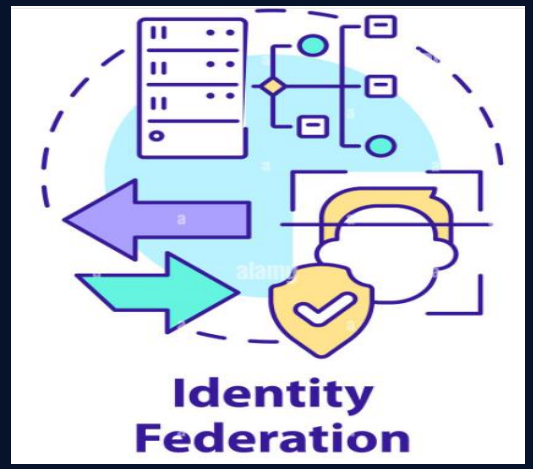
OWASP Top 10 Cloud Security Risks & Mitigations

× **Accountability & Data Risk**: Traditional data center of an organization is under complete control of that organization. Organization logically and physically protects the data it owns. Using a third party to store and transmit data adds in a new layer of risk.

Vendor risk management and accountability

OWASP Top 10 Cloud Security Risks & Mitigations

× **User Identity Federation**: Digital identity is a key part of cybersecurity. It controls vital areas such as privileged access to sensitive resources. As enterprises increase their use of Cloud apps and have data stored across Cloud services, control of access through identity management is crucial.



Implement a modern identity service or platform to provide robust, persistent, verified identity controls

OWASP Top 10 Cloud Security Risks & Mitigations

× **Legal & Regulatory Compliance**: OWASP points out the issues of meeting compliance across geographical jurisdictions. For example, if your organization is based in Europe but you use a U.S. Cloud provider, then it might be difficult to map the compliance requirements of EU-centric data protection, and vice versa.

Use a Cloud vendor who understands and applies solutions for the various data protection laws

OWASP Top 10 Cloud Security Risks & Mitigations

× **Business Continuity and Resiliency**: Outsourcing your IT infrastructure to a third-party Cloud provider increases the risk of attaining business continuity for the simple reason that it is outside your control. An outage of Cloud services can have serious repercussions for a business. When Amazon went down for 13 minutes, they lost an estimated cost of $2,646,501.

You need to make sure that your Service Level Agreements (SLAs) cover data resilience, protection, privacy, and that the vendor has a robust disaster recovery process in place.

OWASP ALGIERS

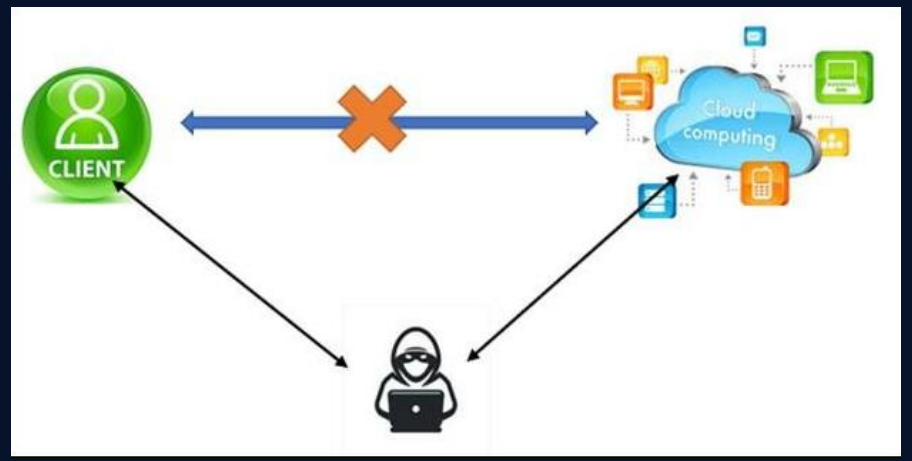
OWASP Top 10 Cloud Security Risks & Mitigations

× **User Privacy and Secondary Usage of Data**: Once data enters the Cloud realm, it is much more difficult to control across its life cycle.

Security awareness training + Compliance frameworks like GDPR.

OWASP Top 10 Cloud Security Risks & Mitigations

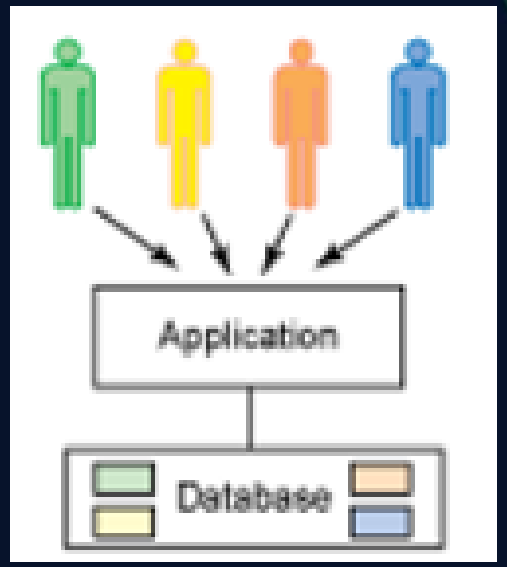
× **Service & Data Integration**: The safe transmission of data is a particular risk in Cloud computing models where it is transmitted over the internet.



Cloud provider should use protocols based on encryption to allow the safe movement of data across an Internet connection.

OWASP Top 10 Cloud Security Risks & Mitigations

× **Multi Tenancy and Physical Security**: Cost savings often dictate that Cloud servers are used in a multi-tenancy setup. This means that you will share server resources and other services, with one or more additional companies. The security in multi-tenancy environments is focused on the logical rather than the physical segregation of resources. The aim is to prevent other tenants from impacting the confidentiality, integrity and availability of data.



Good design + good configuration for the servers for logical separation.

OWASP Top 10 Cloud Security Risks & Mitigations

× **Incident Analysis and Forensic Support**: If a data breach occurs, you must understand how to identify and manage critical vulnerabilities so you respond to the incident as quickly and effectively as possible. Cloud computing can make the forensic analysis of security incidents more difficult. This is because audit and events may be logged to data centers across multiple jurisdictions.

Check out the Cloud vendor policy on handling, evaluating and correlating event logs across jurisdictions.

OWASP ALGIERS

OWASP Top 10 Cloud Security Risks & Mitigations

× **Infrastructure Security**: This covers the entire gamut of how to harden the attack surface of a Cloud infrastructure. It includes configuring tiers and security zones as well as ensuring the use of pre-established network and application protocols. It also includes regular risk assessments with updates to cover new issues.

Put in place various measures to improve general security. For example, privileged access management using robust authentication, secure configuration of server and services, and tiered architecture.

OWASP ALGIERS

OWASP Top 10 Cloud Security Risks & Mitigations

× **Non-Production Environment Exposure Risks**: Need to be accounted for across the entire life cycle of application development and implementation. This includes pre-production environments where design and test activities occur. Because these environments may have less stringent security applied, they may well open up security and privacy risks.

+ In test environments, avoid using real or sensitive data. Ensure that individuals working on the pre-production system have privileged access security measures in place. Make sure to leverage the concept of ‘privacy by design’

OWASP ALGIERS

Conclusion

Conclusion

In conclusion, the landscape of cybersecurity in cloud computing presents both immense challenges and promising solutions.

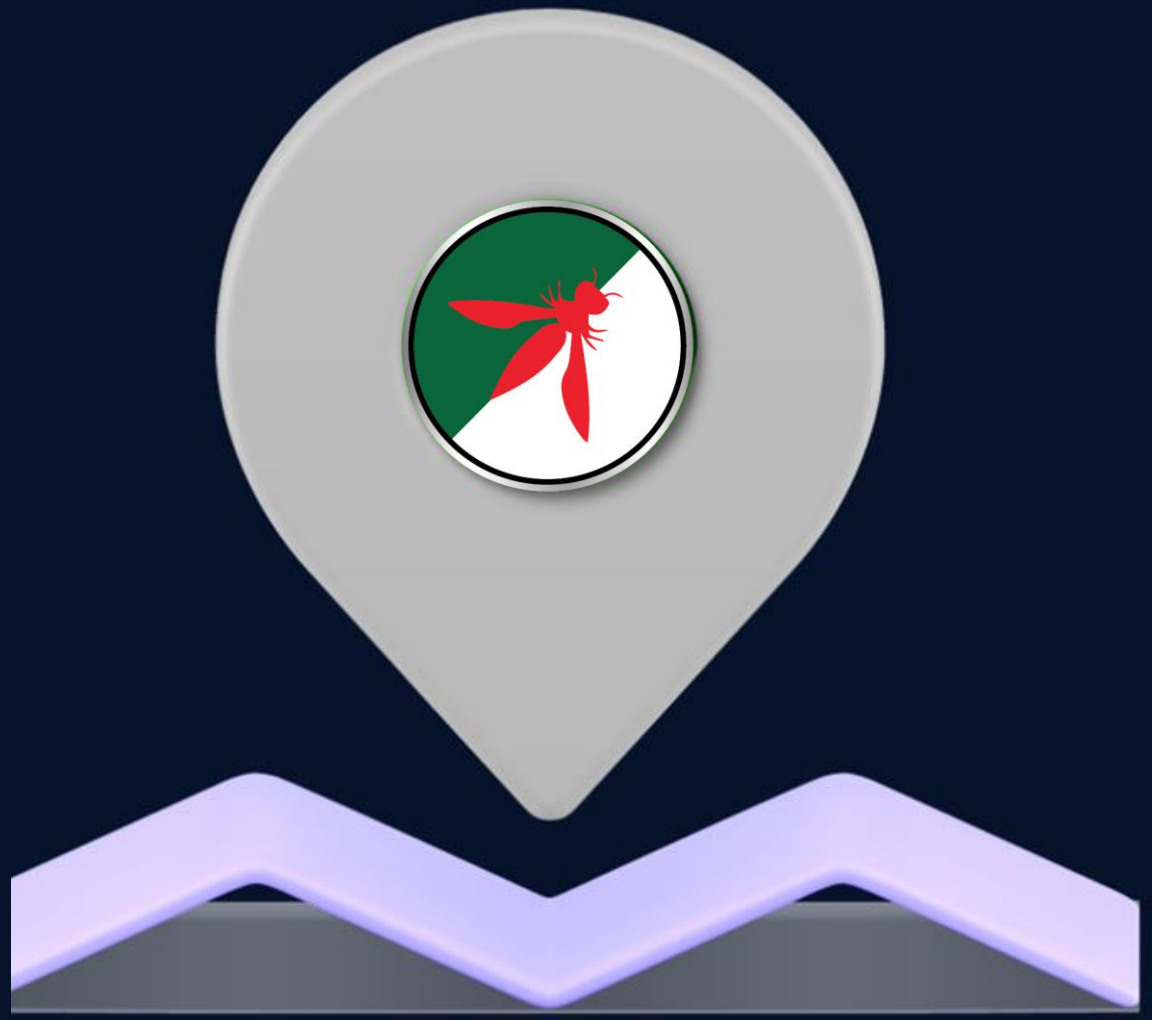
As organizations increasingly migrate their operations to the cloud, they must remain vigilant in addressing the multifaceted threats that accompany this transition.

From data breaches to insider threats, the risks are diverse and evolving.

Thanks For Your Attention!

OWASP ALGIERS

Contact us



ALGIERS-LEADERS@OWASP.ORG

https://owasp.org/www-chapter-algiers/