Cloud Security Series

云计算的安全考虑与措施

Cloud Computing Security Consideration & Measures

Nicolas KE 柯沧海
- Certified Information System Security Professional
- AWS Certified Security Specialty
- AWS Certified Architect – Associate
- AWS Certified Developer - Associate

April 22, 2023

Agenda

- Cloud Computing
- Cloud Security
- Compliance & Regulation
- Conclusion

What is Cloud Computing ?

Instead of buying, owning, and maintaining physical data centers and servers, you can access services, such as computing power, storage, databases, on an as-needed basis from a cloud provider.

- On-demand delivery of IT resources
- Over the Internet
- Pay-as-you-go pricing

Cloud Computing Pros & Cons

- No Upfront Investment
- Cost saving
- Pay As You Go
- Elasticity
- Security Services and Tools

- Security
- No control on data
- Bigger attack surface
- Good internet connection

Security is CIA

- **Availability**: Servers available when you need data & processing
- **Confidentiality**: Data accessed only by authorized people
- **Integrity**: Assurance that data is not modified

Security applied to the cloud

Servers

- Servers are running
- Servers are trusted
- Servers are safe
- Scale up and scale down
- No resource limitation

Data

- Data is safe
- Data is available
- Data not accessible by unauthorized people
- Data not accessible by governments

Connections

- Connections are secured
- Connections are fast
- Efficient firewall
- No DOS / DDOS attack

Shared Responsibility

Customer

Responsible for the applications & data in the cloud

Customer Data

Applications, Access Management

Backups, Certificates, Encryption

Operating Systems, Vulnerability Management, Network traffic, Firewall

Cloud Provider

Responsible for the cloud and its services

Software

Servers | Networking | Storage | Database

Security Services | Backup Services

Infrastructure / Hardware

Data Centers | Edge Locations | Equipments

Server availability & trust: measures

- Auto scaling / Load balancing
- Server with CA certificate
- Data in transit is secure : HTTPS (TLS), SASL, STARTTLS, etc.
- Authentication
- Authorization
- Vulnerability scanning
- Servers correctly patched and configured

Data at rest secure: measures

- Databases in private subnets
  - Bastion host to access them, or not
- Encryption
  - Volume-level, DB-level
  - Column-level encryption
- Data classification
- Authorization
- Integrity check

Mitigating attacks

- Web Application Firewall (level 7)
  - CSRF, XSS, SQL injection
- Anti-DDOS
  - Sudden increase of orchestrated traffic on servers
  - Ping of Doom, Ports,
- Content Delivery Network
  - Software download, cache, acceleration, streaming,
- VPN: encrypted point to point connection
  - Remote Access VPN, Site to Site VPN

Compliance and Regulation

International

- ISO 27001, ISO 27017, ISO 27018
- SOC2
- PCI/DSS

USA

- CLOUD Act
- FISA
- HIPAA
- FISMA
- FedRAMP

EU

- GDPR
- NIS, NIS2
- EU DMA
- EU DSA
- Cyber Resilience Act
- Cyber Solidarity Act

China

- CSL (Cybersecurity Law)
- DSL (Data Security Law)
- MLPS (Multi-Level Protection Scheme)

France

- France: SecNumCloud

Cybersecurity in USA

- CLOUD Act
  - Clarifying Lawful Overseas Use of Data Act
  - Allow US governments to request data from US companies
    - Public safety, terrorism, crime, justice, etc.

Security Frameworks

- HIPAA: Healthcare
- FISMA: Government
- FedRAMP: Government Cloud
- CCPA: California Consumer Privacy Act

Cybersecurity in EU

- GDPR: Personal data protection
  - Cross-border PII data transfer
- Directive NIS2
  - The Network and Information Security (NIS) Directive
  - Categories, subject different supervisory regimes
  - 2eme semester 2024 at the latest

- EU Digital Market Act
- EU Digital Services Act
- Cyber Resilience Act
- Cyber Solidarity Act

SecNumCloud in France

- Origin
  - By ANSSI
  - Certification for trusted cloud service providers
  - Sometimes called “Sovereign clouds”
  - Outscale, OODrive, OVH, Worldline, Orange, etc.
- SecNumCloud
  - ISO 27001 / GDPR
  - Reversibility
  - “Immunité contre les réglementations extra-communautaires”

Cybersecurity in China

- CSL (Cyber Security Law)
  - Real name requirement
  - Data localization, citizen PIIs located in China
  - Prohibited content
  - Technology "backdoors"
  - Critical Information Infrastructure sectors
  - Legal responsibilities
- MLPS (Multi Level Protection Scheme)
  - Protection according to grading
  - Risk control on new technology, Personal Information Protection, Trustable authentication, Security Self Assessment, Detection, Incident Notification
- Critical Information Infrastructure (CII)
  - Communication, energy, transport, water, finance, government, defence

Conclusions

- Cloud computing is irreversible
  - Some reversal movements are only temporary
- Security is a legitimate concern
  - Security is not obscurity
  - Necessary to implement the right security
- Regulation is important
  - Protect national secrets and data
  - Protect citizen data

谢谢！