30-03-2022

GÉANT Cloud Security Checklist

Contents

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).

1 Introduction

In the era of widely used information systems and digital services, cyber security and associated risks are the biggest concern across all business sectors. With the use of external cloud services and moving business processes and data to a cloud provider, this concern is becoming even more critical. Often it presents the biggest barrier to digital transformation and cloud adoption.

The research and education institutions provide a wide range of different information services to their users (researchers, professors, students, staff). They can be organised on internal on-premise equipment, shared with other institutions at the university or NREN level, or outsourced to an external cloud provider. Even though providing the security measures must be shared among all involved stakeholders, while offering the services to its users the biggest responsibilities lie with the institution itself.

The purpose of this document is to help research and education institutions establish appropriate security measures for providing digital services, with special attention to general cloud services. It is organised as a checklist of the most important security-related items, divided into different layers, starting from the physical layer up to the data layer. Depending on the service organisation and implementation, some of the items in the checklist are under the direct responsibility of the service providers, but the role of the institutions is to check and ensure that these measures are in place. Some measures are strictly technical, while equally important are organisational measures, such as policies and procedures, which are mostly under institutional responsibility.

This document can be used as a starting point to help institutions manage various aspects of cloud security, to develop solid security practices or to benchmark the current status of security development and further enhance security strategy.

2 Physical Security

These security measures relate only to on-premise private cloud infrastructure, data centre, network equipment, etc.

- Physical access
  - Policies are in place to provide access to the physical equipment and communication infrastructure or network.
  - Relevant security standards are in place (such as ISO 27001 – Information Security Management, ISO 27017 – Cloud Security, ISO 27018 – Privacy Protection).
  - Monitoring and controls of physical security are in place to prevent unauthorised access (electronic surveillance system, security cards and alarms).
- Asset management
  - Inventory/asset management is in place to keep the list of physical items up to date, with all necessary details.
  - Assets are classified in terms of security and criticality.
- Equipment installation/removal
  - Policy is in place for loading, installing and removing equipment.
  - Old equipment is destroyed in a secure way to assure that its data are permanently destroyed.

3 Network Security

- Configuration and change management
  - Policies are in place to provide smooth and secure changes in network architecture.
  - Configuration management system is in place that provides configuration backup and versioning to a secure location.
- Data confidentiality and integrity in transit across the network on the path from user organisations to cloud provider
  - A policy on the use of cryptographic controls and key management is in place, taking into account information that is critical/less critical to the institution.
  - Remote access to cloud services is provided by using cryptographic functions with key lengths based on common (inter)national security standards.
- Protection against remote attacks
  - Firewall protection is in use.
  - Intrusion detection system is in use, at least for the following attacks:
    - DDoS.
    - Dictionary attack (password guessing).
    - Network/port scanning.
    - Botnet C&C attempt.
  - Measures are in place to mitigate attacks:
    - Manual – well-defined procedure and roles.
    - Automatic – protection system that enforces security policy.

4 Host and Application Security

- Vulnerability management
  - A vulnerability management process is defined, documented and implemented.
  - A person responsible for the vulnerability management process is assigned.
  - Vulnerability assessment is carried out on a regular basis.
  - Periodic penetration testing is organised.
- Patch management
  - A patch management process is defined, documented and implemented.
  - A patch manager responsible for the process is assigned.
  - System software is regularly updated.
  - Security patches, especially those that treat critical vulnerabilities, are deployed in a timely manner.
- Access management
  - Host firewall system is configured with minimum ports opened to support services running.
  - Intrusion detection system is running on the host, monitoring and generating alarms for unauthorised access and login attempts.
- System backup and recovery
  - A policy on system backup and recovery is in use.
  - Automatic system backup is in place at least on a daily basis (single or multiple generation).
  - System backup is stored remotely in a secure way.
  - Recovery procedure is periodically carried out in order to test the backup data consistency.

5 Information Security

- Personal data security
  - A policy for personal data protection is in place.
  - Minimal personal data are required for registration to use the service.
  - User data, including personal sensitive data, can be securely exported by the data owner in an interoperable format.
  - User data, including personal sensitive data, can be securely deleted and permanently destroyed.
  - Data are classified in terms of security and criticality.
- Encryption
  - A policy on data encryption and cryptographic key management is in place.
  - User data are transparently encrypted when stored on the system, with key lengths based on common (inter)national security standards.
  - Tools are in place for user data encryption under full user control, including cryptographic key management based on common (inter)national security standards.

6 Threat Modelling

- Risk management
  - A risk management process is defined, documented and implemented.
  - A risk manager responsible for the risk management process is assigned.
  - Security measures are approved and implemented based on risk assessment.
- Incident management
  - An incident management process, including reporting and escalation approaches, is defined, documented and implemented, with identified responsibilities.
  - A person or team responsible for the incident management process is assigned.
- Business continuity management
  - A business continuity management process is defined, documented and implemented, with identified responsibilities.
  - A person responsible for the business continuity management process is assigned.

7 Legal and Compliance

- Contracts are in place, clearly defining the obligations and responsibilities defined between all involved parties (institution, NREN, cloud provider, managed service provider, third-party experts and suppliers), stating relevant security aspects.
- The contracted jurisdiction area ensures the legal framework which is not on a lower level than the national one.
- Data (original and backup copy) are stored in the country that ensures data protection regulation which is not on a lower level than the national regulation.
- A procedure for data access and processing by law enforcement is clearly defined and acceptable, including the information to which it is allowed and under which conditions.
- Compliance with GDPR rules and principles is in place.
- SLA is clearly defined, with the key performance indicators monitored and reported on a regular basis.

Glossary

C&C	Command and Control
DDoS	Distributed Denial of Service
GDPR	General Data Protection Regulation
ISO	International Organisation for Standardisation
NREN	National Research and Education Network
SLA	Service-Level Agreement