NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Risks Related to Cloud Service Providers

Supply Chain Working Group Guideline

Brenda Davis, CPS Energy

Critical Infrastructure Protection Committee

December 10-11, 2019 | Atlanta, GA

RELIABILITY | RESILIENCE | SECURITY




Supply Chain Risks related to Cloud Service Providers

Introduction

- NIST describes cloud computing[1] as ubiquitous, convenient, on-demand network access to a shared pool of configurable resources.
- As with any new technology, a range of risks and security factors are introduced.
- This guideline is intended to support entities in evaluating supply chain risks associated with vendors providing or utilizing cloud services, however, does not provide compliance guidance.

[1] *NIST SP800-145* NIST Definition of Cloud Computing

Cloud Services Supply Chain Risk Considerations

- **Shared Services** - Cloud services that share resources such as the computing platform or storage with multiple clients.
- **Service Level** – Establish proper service level agreements commensurate with the value or sensitivity of the data.
- **Security Controls** – Determine the demarcation point of security controls between the vendor and the entity.
- **Service Model** – Related to the concept of shared services, the service model chosen (SaaS, IaaS, PaaS) may include risks of layered services with multiple vendors.

Supply Chain Risks related to Cloud Service Providers

Cloud Services Supply Chain Risk Considerations

- **Data Sovereignty** – Data may be restricted legally from being stored in or routed through foreign jurisdictions depending on data classification, sensitivity, ownership and other factors.
- **Regulatory Limitations** – There may be inherent limitations to mitigations that could be applied that must be considered when assessing risks.
- **Verification/ Certifications** – How a vendor may demonstrate and communicate security. For example:
  - ISO/IEC 27001 – Information Security Management Standard
  - NIST SP 800-53 – Security and Privacy Controls for Federal Information Systems and Organizations
  - CSA STAR – Cloud Security Alliance Security Trust Assurance and Risk Program
  - FedRAMP – Federal Risk and Authorization Management Program
  - 3rd Party Attestation - (Example: SOC2, Type 2 attestation)

Supply Chain Risks related to Cloud Service Providers

Cloud Services Supply Chain Risk Considerations

- **Response and Recovery–**
  - Incident response and recovery plans should identify responsibilities and points of contact for both organizations to respond appropriately to security incidents and interruptions of service.
  - The service level agreement should clearly define security incidents and expectations of all parties involved.

Supply Chain Risks related to Cloud Service Providers

APPENDIX A - References, Acronyms and Definitions

Cloud Service Provider[2]	Cloud service providers (CSP) offer network and telecommunication services, infrastructure, or business applications hosted in a data center that can be accessed by companies or individuals using network connectivity.
Cloud Computing[3]	Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.
SaaS **(Software as a Service)[3]**	The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

[2] https://www.sdxcentral.com/cloud/definitions/what-are-cloud-service-providers/

[3] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf)

APPENDIX A - References, Acronyms and Definitions

PaaS **(Platform as a Service)[3]**	The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
IaaS **(Infrastructure as a Service)[3]**	The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

[3] *https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf)*

Supply Chain Risks related to Cloud Service Providers

References

https://www.us-cert.gov/ncas/alerts/TA18-004A (Meltdown and Spectre)
https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf
https://www.naesb.org/
https://www.iso.org/isoiec-27001-information-security.html
https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final
https://www.nist.gov/cyberframework
https://cloudsecurityalliance.org/star/
https://www.fedramp.gov/
https://cloudsecurityalliance.org/articles/cloud-security-alliance-announces-fedstar-a-new-joint- certification-system-with-fedramp/

Example of cloud services infrastructure:

https://azure.microsoft.com/en-us/overview/what-is-saas/

Additional topics and guidance for Supply Chain Security can be found at

https://www.nerc.com/pa/comp/Pages/Supply-Chain-Risk-Mitigation-Program.aspx.

Supply Chain Risks related to Cloud Service Providers

Questions and Answers