NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Security Guideline for the Electricity Sector - Supply Chain

Risks Related to Cloud Service Providers

The objective of the reliability guidelines is to distribute key practices and information on specific issues critical to promote and maintain a highly reliable and secure bulk power system (BPS). Reliability guidelines are not binding norms or parameters to the level that compliance to NERC's Reliability Standards is monitored or enforced. Rather, their incorporation into industry practices is strictly voluntary.

Introduction

Cloud computing offerings, defined as those which enable "ubiquitous, convenient, and on-demand network access to a shared pool of configurable computing resources"[i], have been introduced to the market over the past decade. In some cases, this new model has resulted in the potential to reduce costs and increase efficiency, but as with any major technological change, it also brought a range of risks and security factors to be considered. Recognizing that the electricity subsector is among the potential customer base for many of these new technologies, engagement and partnerships between the vendor community and the electricity subsector are highly important – particularly given the rate at which these technologies and offerings evolve. Vigilance and oversight from all parties are essential to both identify and address risks associated with the paradigm shift.

This guideline presents some supply chain risk considerations associated with cloud computing. It is not intended to endorse hosting Bulk Electric System (BES), BES Cyber Systems (BCS) or BCS Information (BCSI) in the cloud. Rather, this guideline is provided to support entities in their evaluation of the supply chain risks associated with vendors providing or utilizing cloud services.

Cloud Services Supply Chain Risk Considerations

Shared Services - One of the starting points when considering a move into the cloud is to understand the implications of shared services, which share resources such as the computing platform or storage with multiple clients. Understanding the responsibilities of security for the solution being provided is important in assessing risk. Shared services, by their nature, present security challenges not encountered when an organization owns and operates "end-to-end" solutions. For instance, cloud risks exemplified by the *Spectre* and *Meltdown*[ii] vulnerabilities demonstrated how an adversary could obtain confidential information by manipulating shared features of cloud resources, such as storage devices.

When considering the deployment of cloud-based services, the entity is responsible for ensuring that capabilities are maintained for security, change management, and other considerations of the cloud solution. Risks associated with each cloud implementation will depend on the service model chosen as well as the business requirements for confidentiality, integrity, and availability for the application.

Many third-party security service providers and software security brokers offer security oversight and monitoring for cloud services; however, this ultimately adds another layer of supply chain risk in procuring and managing third party services.

Service Level - Cloud service solutions are available in various configurations and may involve multiple tiers of vendors. The service model chosen should be considered and proper service level agreements established commensurate with the value or sensitivity of data being stored. Organizations should clearly understand their tolerance to interruptions in service. The National Institute of Standards and Technology (NIST) provides a number of resources for helping an entity categorize the importance of information being stored in the cloud. For example, NIST publication FIPS 199[iii] uses the security objectives of confidentiality, integrity, and availability to assess risk and categorize information.
Among the practices and controls a vendor and entity should implement are:

- Mitigate the effects of denial of service attacks and unauthorized access to information.
- Ensure individuals who have access protect the information entrusted to them.
- Ensure data is not modified by accidental or unauthorized means. This would include ensuring each client’s data is segregated from other clients’ data.

Security Controls - The entity should determine the demarcation point of security controls between the vendor and the entity to determine the scope of cloud service provider (CSP) security controls and the entity’s security controls for the cloud services. A security controls gap analysis will assist the entity in determining incident response and recovery strategies. Refer to the security frameworks addressed below under “Verifications/Certifications.”

Service Model – CSPs’ service offerings include Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Organizations can select the service model that best satisfies its needs, but it is important to perform due diligence/analysis for services to be provided.

Each layer of cloud services (IaaS, PaaS, and SaaS) may encompass shared responsibility, meaning each layer of the cloud stack may be provided by different vendors. Therefore, a vendor providing cloud services may also be relying on other CSPs to support different service models. For example, an entity could choose a SaaS vendor that is using another vendor for IaaS. Thus, while an entity may think its attack surface includes only the SaaS vendor, there may actually be three vendors providing SaaS, PaaS and IaaS.

An entity should always seek to understand what aspects of the cloud service are being provided by the vendor or CSP and whether third parties are critical to that service delivery. Instituting clauses in contracts or supplements, as well as asking questions in a risk assessment as to the number and types of vendors the service provider uses to provide cloud services, is vital to understanding and addressing the actual risk in the relationship.

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. Such restricted data may reside on servers that are accessible to and monitored by government entities. As a result, organizations should ensure that agreements with CSPs include a high level of transparency. See "Regulatory Limitations" below for additional information.

Regulatory Limitations – While the goal is always to reduce risk, there may be legal constraints that limit the extent to which mitigations can be applied to cloud-based services. Regulations that prohibit the vendor from customizing certain aspects of its service offerings may present inherent limitations to mitigations that could otherwise be applied. One notable example is "eTag" – a specification required by the North American Energy Standards Board.[iv] Consider issues like these when assessing risks.

Verification/ Certifications - How a vendor demonstrates and communicates its security is an important consideration when considering a CSP. Some vendors describe their security programs with references to standards or frameworks such as ISO 27001[v], NIST SP800-53[vi], NIST Cybersecurity Framework[vii], or Cloud Security Alliance (CSA) Security Trust Assurance and Risk (STAR) Program[viii].

Vendors adhering to security standards or frameworks should provide an attestation report from a certified and independent third-party auditor on controls relevant to security, availability, processing integrity, and confidentiality. It is a best practice to ensure the evaluation was conducted according to the rules published by the standard's governing authority. It is also imperative to understand the scope of the products and services that are covered under the certification.

FedRAMP[ix] (Federal Risk Authorization Management Program) is an example of a certification that an organization could use to demonstrate that it has met the requirements of an independent standard. Additionally, FedRAMP and CSA are developing a joint certification system called FedSTAR [x].

Alternatives to the above mentioned certifications or third party attestations include the vendor's assessment of controls in response to an Entity questionnaire or onsite inquiry. A greater level of scrutiny should be applied with the security questionnaire method since it lacks independent verification of the information being provided by the vendor.

It is important to note the direct relationship between the burden of proving security that is placed on vendors and the cost of services. This is an important consideration when choosing the proper verification/certification method. A program like FedRAMP imposes the greatest burden on the vendor, which is attractive from a security standpoint, but could be very costly too. At the other extreme, a security questionnaire can be very cost-effective, but lacks the impartiality of an independent third-party review. In other words, there is a tradeoff between risk and cost associated with all of the verification methods discussed above.

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

For further information and references, visit the NERC Supply Chain Risk Mitigation Program site.[xi]

References, Acronyms and Definitions

- **Cloud Service Provider**[xii]
  - CSPs 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**[xiii]
  - 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)**[xiii]
  - SaaS allows users to connect to and use various types of cloud-based applications over the Internet.[xiv] 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..[xv]
- **PaaS (Platform as a Service)**[xiii]
  - 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.[xvi] 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)**[xiii]
  - 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, deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

[i] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-145 NIST Definition of Cloud Computing
[ii] https://www.us-cert.gov/ncas/alerts/TA18-004A
[iii] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf
[iv] https://www.naesb.org/
[v] https://www.iso.org/isoiec-27001-information-security.html
[vi] https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final
[vii] https://www.nist.gov/cyberframework
[viii] https://cloudsecurityalliance.org/star/
[ix] https://www.fedramp.gov/
[x] https://cloudsecurityalliance.org/articles/cloud-security-alliance-announces-fedstar-a-new-joint-certification-system-with-fedramp/
[xi] https://www.nerc.com/pa/comp/Pages/Supply-Chain-Risk-Mitigation-Program.aspx
[xii] https://www.sdxcentral.com/cloud/definitions/what-are-cloud-service-providers/
[xiii] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
[xiv] https://www.us-cert.gov/ncas/alerts/TA18-004A
[xv] https://azure.microsoft.com/en-us/overview/what-is-saas/
[xvi] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf