Overview of Security in Cloud Computing
Using Cloud Security Alliance (CSA) Guidelines

Sahil Khanna
University of Maryland
College Park, MD
Email: skhanna9@terpmail.umd.edu

Naveen Achyuta
University of Maryland
College Park, MD
Email: naveen92@umd.edu

Susmita Pradhan
University of Maryland
College Park, MD
Email: susmita4@umd.edu

Laveena Dulani
University of Maryland
College Park, MD
Email: laveena.dulani94@gmail.com

Apeksha Chauhan
University of Maryland
College Park, MD
Email: achauha2@umd.edu

ABSTRACT

Cloud technologies brought many opportunities and services on one platform. Cloud Computing enables ubiquitous access to a shared pool of resources. Cloud Computing with time has posed privacy and security concerns. As cloud services are handled by third party service providers, they have access to data that is on the cloud at any point in time. They could accidently or deliberately delete information or share information with other parties or organizations. The issues and opportunities of cloud computing gained considerable notice in 2008 within the information security community. At the ISSA CISO Forum in Las Vegas, in November of 2008, the concept of the Cloud Security Alliance was born. The Cloud Security Alliance promotes implementing best practices for providing security assurance within the domain of cloud computing and has delivered a practical, actionable roadmap for organizations seeking to adopt the cloud paradigm. In this paper. We have summarized these 14 domains and demonstrates the importance, challenges, implementations and risk associated with these domains.

DOMAIN 1: Cloud Computing Concepts and Architecture Models

Introduction

Cloud Computing is the delivery of on-demand computing resources over the internet. Cloud Computing at its essence is transformative and disruptive. The key techniques to create a cloud are abstraction and orchestration. Abstraction is the act of representing essential features of a service without having to include details of the underlying infrastructure. Orchestration is the technique to allocate and deliver a set of resources from the resource pools to the consumer. Cloud services are broadly categorized into service models namely, Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). There is a varying level of abstraction and orchestration employed in each of the service models. The consumer can then choose a suitable service model suitable for his organization.

Importance

- Cloud Computing offers numerous benefits in agility, resilience and economy.
- Organizations can move faster, reduce downtime, save money by migrating their operations into the cloud.
- Cloud Computing offers enhanced and simplified management services through centralized administration, service level and availability backed agreements.

Implementation

A good practice to implement and deploy a cloud based solution would be to follow an implementation plan.

- Decide why you want to use a cloud based solution and how you intend to use it.
- Consider the period for which you want to use the services of a provider.
- Plan out the phases of migration and estimate the period over which you want to achieve it.
- Negotiate the terms of security with the cloud service provider and ensure the compliance standards are met.
- Have a contingency plan ready to deal with any downtime.

Challenges

- Simply moving operations into a cloud provider with no changes will reduce agility, resiliency and security at an increased cost.
- Although service providers provide best security standards, moving data into the cloud can open up security risk in the form of vulnerabilities, loss of data, private information as a result of attacks.
- Infrastructure being managed by the service provider limits the control the user can have over the infrastructure.
- Multi-tenancy in certain solutions result in rigid service levels, and limited customisation.

DOMAIN 2: Governance and Enterprise Risk Management

Introduction

Adoption of a cloud service model or a deployment model by an organization is followed by establishing a governance model or framework that encompass policies, process and control how an organization is run in the cloud. Security in Cloud is concerned with four areas: governance, enterprise risk management, risk management, risk tolerance. Governance and Enterprise Risk Management in the Cloud concern identification and implementation of appropriate organizational structures, processes, controls to maintain effective information security governance, risk management and cost control.

Importance

By adopting a governance model, organizations can:

- Assess and monitor, understand the organization's current cloud landscape.
- Design and enhance by focusing how an organization should govern its cloud solutions to minimize risk.
- Design roles and responsibilities and defining policies, standards and metrics to which all parts of the organization must adhere.
- Build and operationalize by creating processes, metrics, reporting to manage a cloud model and enable IT and business to make informed decisions. As a result, there is a greater transparency, status tracking and reporting.

Challenges

- Traditional IT governance frameworks are not adapted to cloud solutions. This gives rise to the need of new frameworks that address and guide the migration of services into the cloud.
- Businesses units of certain organizations procure IT services of cloud service providers without the involvement of IT departments. This introduces problems in operating such environments and even making it secure. This is known as shadow IT.

Implementations

When choosing a Cloud Service Provider (CSP), an organization can base its decision upon three factors:

- Contracts are a way of determining how a CSP abides by its agreement to provide services. For example, availability, services, scalability,etc
- Supplier Assessments are performed by potential cloud customers. This is a way to evaluate the financial viability, offerings, reputation, feedback of the CSP.
- Compliance Assessments: These are performed by third party auditing firms whose reports determine the CSP's ability to comply with security standards. These reports are usually made available at the request of the potential customer.

A cloud governance model spans the three pillars of people, process and technology and encompass the entire cloud lifecycle, from identification and configuration to migration, management and decommission.

An effective way to implement governance is to develop a Cloud Governance Framework/ Model as per industry best practices, global standards, regulations like CSA CCM, COBIT 5, NIST
RMF, ISO/IEC 27017, HIPAA, PCI DSS, EU GDPR, etc. When adopting a framework or a model, an organization should also address the risk involved and have contingency and incident response plans in place.

Risk Associated with noncompliance

In absence of a strong governance framework:

- An organization would experience failed migrations. There lies a possibility of data breach, increased vulnerabilities, cost overruns, complexity.
- Vendor Lock In can be another consequence the absence of an exit strategy and service portability would make migrating to another cloud service provider impossible.
- The SLAs might not be in alignment with the company's expectations which then hinders with smooth operation in the cloud.

DOMAIN 3: Legal Issues, Contracts and Electronic Discovery

Introduction

Contracts are a written agreement between two participating entities and are enforceable by law. A contract between a cloud user and a cloud service provider would describe the usage of services, service level agreements, data security, data privacy that are in accordance with the federal laws of the country or region the services would be operated in. Migration of an organization's operations into the cloud could possibly run into legal issues. This domain describes legal issues pertaining to migration of data in the cloud. Contracting with cloud providers, and handling discovery in case of a legal proceeding.

Importance

- Cloud customers should understand the legal implications of using the services of a cloud provider and ensuring that the organization follows the guidelines that ask it to follow data protection policies.
- It is essential for the entities that participate in contractual agreements to understand the legal implications in case of failure to adhere to an agreement.
- Cloud customers should have a clear understanding of the legal and technical requirements to meet any electronic discovery requests in case of a legal proceeding.
- Cloud providers should reveal their policies, requirements and terms of their contract to their potential customers in order to refrain from legal procedures.

Implementations

Legal Frameworks Across the Globe

A Cloud Service Provider provides its services to consumers across the globe. A lot of countries have adopted legal frameworks that require organizations to safeguard the privacy of personal data and security information and require notifying the consumer in event of a breach.
United States employ federal laws such as Gramm-Leach-Biley Act, Health Insurance Portability and Accountability Act, Children's Online Privacy Protection Act that safeguard personal information.
In addition to federal laws, U.S states employ laws pertaining to data privacy and data security.
Government agencies also conduct enforcement actions against those companies whose privacy or security practices are inconsistent.

Contracts

Cloud customers may have a contractual obligation to protect the personal information of their own clients, contacts or employees to insure data is not used for secondary purposes. Following are the measures to consider when agreements or contracts are being formed or negotiated.

- Internal Due Diligence: Before entering into a cloud computing arrangement, A cloud customer should investigate whether it has entered into any confidentiality agreements or data use agreements that might restrict the transfer of data to third parties.
- Monitoring, Testing and Updating: Cloud services should be periodically monitored to ensure required security measures are followed. If not, there lies a need to do so.
- External Due Diligence: Practices such as reviewing reports of litigation filed against cloud providers and conducting online searches to evaluate a vendor's reputation may also prove beneficial in the process of negotiations.
- The proposed contact should always be reviewed carefully, even if one is told that it is not negotiable. It might be possible to negotiate changes.

Electronic Discovery

If for some reason, say a breach of contract, dissatisfaction with service agreement, data breach or inability to provide adequate services, there are laws governing discovery.
Summarizing the laws that circle around discovery, a cloud customer and a cloud provider should adhere to the laws of data possession, custody and control. Whether or not either of the party is obligated to produce information that it possesses or controls.

Challenges

- Developing legal frameworks, regulations and laws ensuring data is a cumbersome process that needs to consider crucial aspects of cloud service agreements and the roles and responsibilities of participating entities.
- Contract negotiations involve revision of terms of agreement over and over again. This process takes time and is required to ensure that agreement to one of the terms doesn't compromise the implementation of other terms that the organization is required to adhere to.
- In cases where the company is bound by nondisclosure agreements, legal proceedings might experience a roadblock.

DOMAIN 4: Compliance and Audit Management

Introduction

The migration of operations to the cloud brings challenges in delivering, measuring and communicating compliance across multiple jurisdictions. Understanding the interaction of cloud computing and regulatory environment is a key component of cloud strategy. In addition, the strategy emphases the attention to cross-border jurisdiction, assignment of responsibilities between providers and users, and capability to demonstrate compliance by providing production evidence and process compliance.

This domain assures adherence to the regulations, policies, agreements and systems. It is divided into two categories. The compliance management assess the state of awareness and adherence, the risks and potential costs of non-compliance whereas audits management is a key tool for assuring compliance.

Compliance Management

In cloud environment both providers and customers share the responsibilities to comply with regulations, however, customers are the ultimately responsible for their compliance. These responsibilities are defined through contracts, assessments and specifics of the compliance requirements. Many cloud providers are certified for various regulations and industry requirements, such as PCI DSS, SOC1, SOC2, HIPAA, best practices like CSA CCM, and global regulations like the EU GDPR. The customer is still ultimately responsible for maintaining the compliance of what they build and manage. For example, if an IaaS provider is PCI DSS-certified, the customer can build their own PCI-compliant service on that platform and the provider's infrastructure and operations should be outside the customer's assessment scope. However, the customer can just as easily run afoul of PCI and fail their assessment if they don't design their own application running in the cloud properly.

Audit Management

In cloud environment, cloud customers may be used to auditing third-party providers, but the nature of cloud computing and contracts with cloud providers will often preclude things like on-premises audits. On-premise audits can be considered as a security risk when providing multi-tenant services. Customers working with these providers will have to rely more on third-party attestations rather than audits they perform themselves. Even depending on the audit standard, actual results may only be releasable under a nondisclosure agreement (NDA), which means customers will need to enter into a basic legal agreement before gaining access to attestations for risk assessments or other evaluative purposes. This is often due to legal or contractual requirements with the audit firm. Cloud providers should understand that customers still need assurance that the provider meets their contractual and regulatory obligations, and should thus provide rigorous third-party attestations to prove they meet their obligations.

Importance

- It assures the compliance to government regulations, and standards
- It helps in risk governance, and initiate corrective actions
- It improves the internal and external processes of both cloud providers and customers
- It increases the efficiency and reliability by systematic implementation of processes
- It reflects the best practice, appropriate resources, and tested protocols and standards

Challenges

- Understanding their full compliance obligations before deploying, migrating to, or developing in the cloud.
- Evaluating provider's third-party attestations and certifications and align those to compliance needs.
- Understanding the scope of assessments and certifications, including both the controls and the features/services covered.
- Managing compliance and audits over time i.e. compliance, audit, and assurance should be continuous.
- Working with regulators and auditors who may lack experience with cloud computing technology.
- Working with providers who may lack audit and regulatory compliance experience.
- Keep a register of cloud providers used, relevant compliance requirements, and current-status.

Implementations

Compliance management is a process to adhere to regulations. One the example could be CSA Consensus Assessments Initiative Questionnaire filled by Amazon Web Services which provides wide variety of questions which can help to assess the security policies.
Figure 1 First row of CSA AWS Assessment for compliance management [2]
The implementation of the audit management is achieved by creating Artifacts. Artifacts are the logs, documentation, and other materials needed for audits and compliance; they are the evidence to support compliance activities. Both providers and customers have responsibilities for producing and managing their respective artifacts.
Figure 2 Examples of Artifacts [1]
Customers are ultimately responsible for the artifacts to support their own audits, and thus need to know what the provider offers, and create their own artifacts to cover any gaps. For example, by building more robust logging into an application since server logs on PaaS may not be available.

Risk Associated with noncompliance

Noncompliance to government standards and regulation leads to legal actions against the company. Thus, companies operated in different regions should be aware of the regulations of that regions and should implement processes to comply to the regulations and standards. For example, companies operating in US should adhere to HIPAA (requires healthcare providers to protect patient data) if they are dealing with patients' data or PCI DSS (requires anyone who accepts credit cards to protect cardholder data) if they are dealing with credit cards data.

DOMAIN 5: Information Governance

Introduction

Information Governance is defined by CSA as "Ensuring the use of data and information complies with organizational policies, standards and strategy including regulatory, contractual, and business objectives" [1].

Information Governance is a broad topic, we have focused the scope of this domain to information security in this paper. The primary goal of information security is to protect the fundamental data that supports the systems and applications. As companies transition to cloud computing, challenges like elasticity, multi-tenancy, new physical and logical architectures, and abstracted controls require new data security strategies.

Importance

This domain plays a significant role in data governance. Information governance defines many governances for hosting data in cloud. These different governances assure data security in cloud. Some of the governance considerations are mentioned below.

- **Information Classification**: It is tied to compliance and affects cloud destinations and handling requirements.
- **Information Management Policies:** It should also cover the different SPI tiers, since sending data to a SaaS vendor versus building your own IaaS app is very different.
- **Location and Jurisdiction Policies**: All hosted data must comply with locational and jurisdictional requirements.
- **Ownership**: It allocate the ownership of data when hosted on cloud.
- **Custodianship:** When data hosted on cloud then cloud provider becomes the custodian, but the data encryption is still under custodianship of the organization.
- **Privacy**: It consists of regulatory requirements, contractual obligations, and commitments to customers. You need to understand the total requirements and ensure information management and security policies align.
- **Contractual controls**: It is your legal tool for extending governance requirements to a third party, like a cloud provider.
- **Security controls**: These are the tool to implement data governance.

Compliance of these domains is very important in information governance to host data securely on the cloud.

Challenges

There are numerous factors which effects the information and data governance in the cloud.

- **Multitenancy:** The shared resource pool among different unknown users requires information governance needs. A poor implementation of information governance makes system vulnerable to cyberattacks.
- **Shared Security Responsibilities:** The shared resource pool comes with the shared responsibility. It is very important to identify difference between the ownership and custodianship of data in the cloud. The terms basically require recognizing who owns the data and who manage the data according to the contracts, for example if you are hosting data in public cloud, then provider will be custodian. Unclear responsibilities may lead to poor regulatory compliance.
- **Jurisdictional boundaries:** Cloud provides the capability to store data in multiple region which requires to understand the location specific policies. Lack of knowledge may compromise the data in certain regions.
- **Compliance, regulations, and privacy policies:** These may be impacted by cloud due to the combination of a third-party provider and jurisdictional changes, e.g., your customer agreement may not allow you to share/use data on a cloud provider, or may have certain security requirements (like encryption).
- **Destruction and removal of data:** Customer and provider need to ensure the destruction and removal of data in accordance with policy. If this governance is not in place, it may leads to data leaks or loss.

Implementations

The governance can be implemented using data security lifecycle, it helps to understand the security boundaries and controls around the data. The lifecycle includes six phases from creation to destruction. The knowledge of phases and location makes it easy to secure the data and form a systematic process.
Figure 3 The data security life cycle [1]

- **Create**: Creation is the generation of new digital content, or the alteration/updating/modifying of existing content.
- **Store**: Storing is the act committing the digital data to some sort of storage repository and typically occurs nearly simultaneously with creation.
- **Use:** Data is viewed, processed, or otherwise used in some sort of activity.
- **Share**: Information is made accessible to others, such as between users, or to customers.
- **Archive**: Data leaves active use and enters long-term storage.
- **Destroy**: Data is permanently destroyed using physical or digital means.

One of the example would be provision of encryption in Amazon Elastic Block storage and deletion of data when the user releases the resources.

Risk Associated with noncompliance

- **Regulatory Requirements:** Many organizations face requirements for retention of information, controlling data generation processes, managing electronic records and signatures due to government regulation. Noncompliance may lead to legal action.
- **E-discovery/ESI Compliance:** ESI is a term that is used in the industry to refer to electronic records, data, and information that is a potential target for expected or existing litigation. E-discovery is the process for searching or collecting electronic information that may be subject to a legal hold, so it is predominantly US organizations that face these risks. A legal hold requires that an organization communicate to parties the potentially created or managed information that is important to supporting or refuting a litigation matter such that they do not alter nor destroy the information that is included in the description of the hold.
- **Data Management, Migration & Integration**: If you are not managing retention and you don't have strong metadata or data governance requirements to store big data on cloud, all of this data is not living up to its potential, and thus, the real benefits of your cloud deployment will not be realized.

DOMAIN 6: Management Plane and Business Continuity

Management Plane

Introduction

The management plane is the single most significant security difference between traditional infrastructure and cloud computing. The tools and interfaces we use to manage our infrastructure, platforms, and applications, form a part of the management plane. Cloud abstracts and centralizes administrative management of resources. Centralization also brings security benefits, like – no hidden resources and open configuration specifications. Management planes allows for the control of data center configuration using API calls and web consoles, in place of boxes and wires. Access to the management plane is like

unfettered access to your data center, obviously with required security policies that limit access to the management plane.
The management plane refers to the interfaces for managing your assets in the cloud. If you deploy virtual machines on a virtual network the management plane in how you launch those machines and configure that network. For SaaS, the management plane is often the "admin" tab of the user interface and where you configure things like users, settings for the organization etc. The management plane controls the metastructure and is also part of the metastructure itself.
Management consolidates many things that were previously managed through separate systems and tools, and then makes them internet accessible with a single set of authentication credentials. Management plane is like an extension if the shared responsibility model. The responsibilities of cloud the provider and cloud user for the management plane are delineated below:

- The cloud provider is responsible for ensuring the management plane is secure and necessary security features are exposed to the cloud user, such as granular entitlements to control what someone can do even if they have management plane access.
- The cloud user is responsible for properly configuring their use of the management plane, as well as for securing and managing their credentials.

Importance

- Management plane allows for centralization of resources.
- Management plane is a key tool for enabling and enforcing separation and isolation in multi tenancy. Limiting who can do what with the APIs is one important means of segregating out customers, or different users within a single tenant.
- Management plane makes the cloud infrastructure more secure, which can be achieved using Identity and Access Management (IAM) which includes identification, authentication, and authorizations.

Challenges

- The biggest challenge with management plane is that since it gives centralized access to the cloud resources, it is extremely important to have required security provisions in place. If not, then all the users can have access to all the resources.
- Since management secures cloud infrastructure by Identity access management, it is important that users don't lose their credentials and ensure to create strong password.
- No matter the platform or provider there is always an account owner with super-admin privileges to manage the entire configuration. This should be enterprise owned, tightly locked down and nearly never used. These privileges should be used in smaller groups since, compromise or abuse of one of these accounts could allow someone to change or access essentially everything and anything.

Implementation

All the Software as a service (SaaS) applications like Salesforce.com and Netflix use management plane for their application. Following are the major factors for building and managing a secure management plane:

- **Perimeter security:** Protecting from attacks against the management plane's components itself, such as the web and API servers. It includes both lower-level network defenses as well as higher-level defenses against application attacks.
- **Customer authentication:** Providing secure mechanisms for customers to authenticate to the management plane. This should use existing standards (like OAuth or HTTP request signing) that are cryptographically valid and well documented. Customer authentication should

support MFA as an option or requirement.

- **Internal authentication and credential passing:** The mechanisms your own employees use to connect with the non-customer-facing portions of the management plane. It also includes any translation between the customer's authentication and any internal API requests. Cloud providers should always mandate MFA for cloud management authentication.
- **Authorization and entitlements:** The entitlements available to customers and the entitlements for internal administrators. Granular entitlements better enable customers to securely manage their own users and administrators. Internally, granular entitlements reduce the impact of administrators' accounts being compromised or employee abuse.
- **Logging, monitoring, and alerting:** Robust logging and monitoring of administrative is essential for effective security and compliance. This applies both to what the customer does in their account, and to what employees do in their day-to-day management of the service. Alerting of unusual events is an important security control to ensure that monitoring is actionable, and not merely something you look at after the fact. Cloud customers should ideally be able to access logs of their own activity in the platform via API or other mechanism in order to integrate with their own security logging systems.

Business Continuity and Disaster Recovery in Cloud

Introduction

Business Continuity and Disaster Recovery (BC/DR) is just as important in cloud computing as it is for any other technology. Following are the important aspects of BC/DR in the cloud:

- Ensuring continuity and recovery within a given cloud provider. These are the tools and techniques to best architect your cloud deployment to keep things running if either what you deploy breaks, or a portion of the cloud provider breaks.
- Preparing for and managing cloud provider outages. This extends from the more constrained problems that you can architect around within a provider to the wider outages that take down all or some of the provider in a way that exceeds the capabilities of inherent DR controls.
- Considering options for portability, in case you need to migrate providers or platforms. This could be due to anything from desiring a different feature set to the complete loss of the provider if, for example, they go out of business or you have a legal dispute.

Importance

- **Availability**: The number of Cloud Service providers are increasing by the day. Therefore, the cloud based business continuity solution is available even in remote geographical areas of most countries. The wide range of services on offer means a business gets to cherry-pick the required services to suit its business needs.
- **Cost effective:** The cloud based business continuity solution has been one of the most cost-effective solutions devised till date. Even small businesses can afford such services. The business needs only to pay for the services it uses. In case it needs additional services or needs to scale up current services, it can be easily done, and they need to pay only when used. Knowing that such services are available on-call, as a back-up, means businesses do not need to maintain costly off-site production centers.
- **Easy back-ups:** Data can be backed up to the cloud in real-time or at predetermined intervals to suit business needs. This can be done automatically by programming the servers accordingly. The daily routine of a night-time backup is fast becoming a thing of the past.
- **Easy to restore from the cloud:** In the event of a Disaster, recover and restore functions are easily done. The reliability of using the cloud is greater than 99%. In traditional modes of back-up

such as tapes, disks, flash drives etc. when restore is attempted; the chances are greater of data being corrupted when compared to the cloud.

- **Can be accessed from anywhere:** One of the biggest advantages of using the cloud for Business Continuity is that it can be accessed from anywhere in the event of a disaster. All that is needed is an internet connected device. Of course, security being a prime consideration, proper authentication procedures must be followed. If the production center is out of action, then authorized staff can work from home, hotels, convention centers etc. This wide accessibility gives IT Staff more breathing space to normalize functions and to ensure Business Continuity.

Challenges

Following are the challenges while implementing BC/DR:

- Not all assets need equal continuity.
- Planning for full provider outage can be challenging because of the perceived loss of control. One should look at historical performance.
- Designing for RTOs (Recovery Time Objective) and RPOs (Recovery Point Objective) equivalent to traditional infrastructure can be challenging.
- Planning for cloud provider outages is difficult, due to the natural lock-in of leveraging a provider's capabilities. Sometimes you can migrate to different portion of their service, but in other cases an internal migration simply isn't an option, or you may be totally locked in.
- Business Continuity for private cloud and providers, completely relies on the provider's shoulders, and BC/DR includes everything down to the physical facilities. RTOs and RPOs will be stringent, since if the cloud goes down, everything goes down.

Implementation

One of the implementations of BC/DR is "Chaos Engineering", which is often used to help build resilient cloud deployments. Since, everything in cloud is API-based, chaos engineering uses tools to selectively degrade portions of the cloud to continuously test business continuity. Netflix introduced the application and is popularly known as "Chaos Monkey".

Before implementing BC/DR, the following logical stack must be accounted for:

- **Metastructure:** Since cloud configurations are controlled by software, these configurations should be backed up in a restorable format. This isn't always possible, and is pretty rare in SaaS, but there are tools to implement this in many IaaS platforms (including third-party options) using *Software-Defined Infrastructure*.
- **Software-Defined Infrastructure**: allows you to create an infrastructure template to configure all or some aspects of a cloud deployment. These templates are then translated natively by the cloud platform or into API calls that orchestrate the configuration.
- **Infrastructure:** As mentioned, any provider will offer features to support higher availability than can comparably be achieved in a traditional data center for the same cost. But these only work if you adjust your architecture. "Lifting and shifting" applications to the cloud without architectural adjustments or redesign will often result in lower availability.
- **Infostructure:** Data synchronization is often one of the more difficult issues to manage across locations, even if the actual storage costs are manageable. This is due to the size of data sets (vs. an infrastructure configuration) and keeping data in sync across locations and services, something that's often difficult even in a single storage location/system.
- **Applistructure:** Applistructure includes all the above, but also the application assets like code,

message queues, etc. When a cloud user builds their own cloud applications they're usually built on top of IaaS and/or PaaS, so resiliency and recovery are inherently tied to those layers. But Applistructure includes the full range of everything in an application.

Risk associated with Non- Compliance

Following are the risks associated from non-complying with Business Continuity and Disaster Recovery framework from the Financial Ministry's perspective, but these risks can be extrapolated to other private and public organizations:

1. **Financial Risks:** Financial loss is a major risk when it comes to not having a business continuity plan in place. Almost any workplace disruption that results in downtime for businesses can result in financial loss. Having a business continuity plan that covers all bases can help to reduce that amount of downtime by being able to quickly guide you through how to handle the situation. Depending on the severity of the situation, your company could also be liable which would end up costing you even more.
2. **Operational Risks:** a range of threats from loss of key personnel, settlement failure, and compliance failure, to theft, systems failure and building damage— BC/DR aims to ensure the integrity and quality of the operations of ministry of finance and treasury using a variety of tools including audit, recruitment policies, system controls, and business continuity planning.

DOMAIN 7: Infrastructure security

Introduction

Infrastructure security is the security provided to protect critical infrastructure such as network communications, media etc. Infrastructure security seeks to limit the vulnerability of the network infrastructures and systems to sabotage and contamination. Critical infrastructures naturally utilize information technology as this capability has become more and more available. As a result, network infrastructures have become highly interconnected, and interdependent. Intrusions and disruptions in one infrastructure might provoke unexpected failures to others.

Importance

CSA guidelines are mainly focusing on cloud consideration for the underlying infrastructure, and security for virtual networks and workloads. All clouds utilize some form of virtual networking to abstract the physical network and create a network resource pool. Typically, the cloud user provisions desired networking resources from this pool, which can then be configured within the limits of the virtualization technique used. Many of the cloud computing associated risks are not new and can be found in the computing environments. There are many companies and organizations that outsource significant parts of their business due to the globalization. It means not only using the services and technology of the cloud provider, but many questions dealing with the way the provider runs his security policy determines the network infrastructure security.

Challenges

- **Virtual applications** face considerable challenges to implement since these can become bottlenecks since they cannot fail open, and must intercept all traffic. Virtual appliances should also be aware of operating in the cloud, as well as the ability of instances to move between different geographic and availability zones.
- **Auto Scaling:** Virtual appliances should support auto-scaling to match the elasticity of the resources they protect. Depending on the product, this could cause issues if the vendor does not support elastic licensing compatible with auto-scaling. Virtual appliances may take significant resources and increase costs to meet network performance requirements.
- **Network communication** in the cloud has security vulnerabilities introduced by shared communication infrastructure and virtual networks, but it also faces challenges from conventional IT communication attacks, such as denial-of-service, man-in-the-middle and eavesdropping attacks. Security issues will certainly represent a potential factor to discourage adopters of network virtualization, at least in an initial phase.
- **Interoperability:** Many Virtual Networks will span multiple network infrastructure domains. Interoperability is a crucial requirement to enable widespread deployment of network virtualization. Standardization will be required to enable interoperability between VNs, as well as interoperability between virtualized and non-virtualized networks. In addition, interoperability between VNOs and InPs will also be required, through standardized vertical interfaces.

Implementations

Google Cloud Platform has implemented infrastructure security as a part of their global scale technical security for information processing through their entire lifecycle of information processing at Google. This infrastructure provides secure deployment of services, secure storage of data with end-user privacy safeguards, secure communications between services, secure and private communication with customers over the internet, and safe operation by administrators. Google uses this infrastructure to build its internet services, including both consumer services such as Search, Gmail, and Photos, and enterprise services such as G Suite and Google Cloud Platform. The security of the infrastructure is designed in progressive layers starting from the physical security of data centers, continuing to the security of the hardware and software that underlie the infrastructure, and finally, the technical constraints and processes in place to support operational security.

Risk Associated with noncompliance

In September 2014, theft of credit/debit card information of 56 million customers happened in Home Depot, its POS systems had been affected with malware. A unique custom-built malware had been used.

DOMAIN 8: Virtualization and Containers

Introduction

Virtualization is a technique, which allows sharing a single physical instance of a resource or an application among multiple customers and organizations. It does by assigning a logical name to a physical storage and providing a pointer to that physical resource when demanded. There are different types of virtualization techniques, hardware virtualization, operating system virtualization, server virtualization, storage virtualization to name a few.

Importance

Virtualization security in cloud computing still follows the shared responsibility model. The cloud provider will always be responsible for securing the physical infrastructure and the virtualization platform itself. Meanwhile, the cloud customer is responsible for properly implementing the available virtualized security controls and understanding the underlying risks, based on what is implemented and managed by the cloud provider. For example, deciding when to encrypt virtualized storage, properly configuring the virtual network and firewalls, or deciding when to use dedicated hosting vs. a shared host.

Challenges

Possibly the greatest issue facing virtualization as it applies to Cloud Computing is that economics tends to favor multi-tenancy which essentially means that VMs belonging to multiple customers will likely reside on a common host (at least at some point.) Customers often fear that their most valued intellectual property could be running right next to a server of their fiercest competitor. Guaranteeing security in such circumstances remains a stumbling block to Cloud adoption, but this certainly could be relieved to an extent by paying a premium to guarantee that one's VMS would run on dedicated, isolated hosts. This could represent the ultimate "Private Cloud" where an organization can take advantage of the benefits of Public Cloud without sacrificing security.

- **Certifying and accrediting vendors:** Agencies may not have a mechanism for certifying that vendors meet standards for security, in part because the Federal Risk and Authorization Management Program had not yet reached initial operational capabilities.
- **Additional, unanticipated costs:** The virtual solution costs more than the physical problem.
- **Additional costs often result from implementing OS virtualization:** New hardware and software licenses can be required to solve problems with availability, performance, and management. As VMs burden the existing infrastructure, requirements grow for app and storage networks.
- **Management complexity:** Management tools don't work together. Managing VMs as part of the complete management solution can be a struggle. This includes managing the VMs themselves as well as managing all parts of the data center as one delivery unit. The hypervisor and the host system are two new components that are not part of existing data center management solutions. It is important to be able to manage these devices and understand their impact on performance. Built-in management tools for VM platforms only manage the virtual resources and do not consider any external information.

Implementations

CITRIX virtualization: Citrix XenServer is a leading virtualization management platform optimized for the application, desktop and server virtualization infrastructures. Consolidation and containment of workloads on XenServer enable organizations of any vertical or size to transform their business IT compute infrastructures. XenServer is a comprehensive server virtualization platform with enterprise-class features built in to easily handle different workload types, mixed operating systems and storage or networking configurations. IT gets the benefit of features unique to XenServer such as enhanced virtualized graphics with NVIDIA and Intel and enhanced workload security with Direct Inspect APIs all of which reduce virtual infrastructure costs and complexity.

Risk Associated with noncompliance

OneLogin On May 31, 2017: OneLogin, a San Francisco-based company that allows users to manage logins to multiple sites and apps through a cloud-based platform, has reported a troubling data breach. OneLogin provides single sign-on and identity management for about 2,000 companies in 44 countries, over 300 app vendors and more than 70 software-as-a-service providers. A threat actor obtained access to a set of AWS keys and used them to access the AWS API from an intermediate host with another, smaller service provider in the US.

DOMAIN 9: Incident response

Introduction

Incident response is a term used to describe the process by which an organization handles a data breach or cyber-attack, including the way the organization attempts to manage the consequences of the attack or breach (the “incident”). Ultimately, the goal is to effectively manage the incident so that the damage is limited and both recovery time and costs, as well as collateral damage such as brand reputation, are kept to a minimum.

Importance

Most organizations have some sort of IR plan to govern how they will investigate an attack, but as the cloud presents distinct differences in both access to forensic data and governance, organizations must consider how their IR processes will change. Incident response plans help minimize business risks, and they're mandatory in today's computing environments. Arguably the most important aspect of incident response documentation is the process of determining what constitutes an "incident."

Challenges

Plans are not tailored to the agency. Many organizations implement boilerplate incident response plans that enumerate, in extensive detail, every step that should be taken to investigate a potential incident. While this may feel thorough and reassuring, it can often overcomplicate response procedures and slow down or work against investigations. Off-the-shelf plans are often outdated

and ineffective against evolving threats and changing technology. Plans are only used in real-world incidents. In information security, planning only goes so far. Organizations create comprehensive incident response plans but sometimes do not test them until a real event occurs, only to find they fail at the first step. Ultimately, the incident response team struggles to assess the impact, contain the damage, and communicate to management. The incident response team lacks authority and visibility in the organization. Political disputes can work against the incident response team's efforts, waylay the response process, and prevent timely incident resolution. It is rare that incident response teams operate with the ultimate authority to make the business changes to secure the organization. Rather, they must escalate issues to management to receive the necessary traction, sometimes as incidents worsen.

Implementation

AWS:

AWS has an incident response plan to secure its cloud infrastructure which is specific to the cloud. Through tools such as AWS Cloud Trail, Amazon Cloud Watch, AWS Config, and AWS Config Rules, we track, monitor, analyze, and audit events. If these tools identify an event, which is analyzed and qualified as an incident, that "qualifying event" will raise an incident and trigger the incident management process and any appropriate response actions necessary to mitigate the incident.

Key Benefits of SecureWorks' Incident Response Plan Service:

- Minimize impact and duration: Respond swiftly with a blueprint for action.
- Apply best practices: Ensure that incident response plan has all the key elements.
- Accelerate IT maturity: a tailored game plan that heightens your team's capabilities.

Risk Associated with noncompliance

Gawker Media's had a security breach in which compromised up to 1.4 million accounts. The company was unprepared to respond to an attack in which user data and passwords were posted to peer-to-peer file-sharing networks.

Generally, those breaches where an organization has a security incident response plan in place unravel (publicly and internally) in a manageable and coherent way A breach is identified, investigated, and notifications and remediation services (if relevant) are sent to all those affected. Everyone starts to panic: the breached organization, its partners, and the affected customers. If the situation is bad enough even law enforcement and regulators will get vocal.

DOMAIN 10: Application Security

Introduction

Application security is the use of hardware, software and procedural methods to protect from external threats. It is evolving at a great rate as application development continues to progress and adopt new processes, patterns, and technologies. One of the major reasons that application security is gaining so

much importance is because of cloud computing. Application security is an integral component of software development and IT teams who want to securely build and deploy applications in cloud environments, especially PaaS and IaaS. At present, cloud-based applications are growing rapidly due to the emergence of Internet of Things (IoT). It has been estimated by Gartner that 20.4 billion devices will be connected by 2020 which means most of the crucial application data will be stored in the cloud. Therefore, it has become a necessity to secure the cloud-based applications. Security measures built into applications and reasonable application security routine would minimize the likelihood that unauthorized code will be able to manipulate applications to access, steal, modify, or delete sensitive data.

Importance

For application security in the cloud, some of the existing practices, processes and technologies must be modified to suit its needs. Following are some of the features that help to secure applications in the cloud:

- **Higher baseline security**: Cloud providers have better economic incentives to maintain higher baseline security than other organizations. If there is a baseline security failure, they would jeopardize the trust that the cloud provider needs to maintain with the customer.
- **Isolated environments**: Cloud applications can leverage the technology of virtual networks for hyper-segregated environments. For example, the ability of an attacker to use compromised applications to attack others behind the security firewalls can be eliminated by deploying multiple application stacks on different virtual networks.
- **Independent virtual machines**: Application security can be enhanced by using micro-service architectures. Since cloud doesn't require the consumer to optimize the use of physical servers, a requirement that often results in deploying multiple application components and services on a single system, developers can instead deploy more, smaller virtual machines, each dedicated to a function or service. This reduces the attack surface of the individual virtual machines and supports more granular security controls.
- **Unified interface**: A unified interface (management interface and API) for application services provides a more comprehensive and better management than the traditional devices like servers, firewalls, and ACLs which are usually managed by different groups. Therefore, unified interface helps to reduce security failures that are caused due to lack of communication or full-stack visibility.

Challenges

Following are the some of the challenges on application security that the cloud providers will face:

- **Increased application scope**: Cloud applications are often connected with the management plane to trigger automated actions, especially in PaaS. Security failure of the management plane can affect the security of applications associated with that cloud account. Also, developers and other teams would have to be given access to management plane as opposed to always going through a different team which handles it. Data and sensitive information will be exposed within management plane. Therefore, failure of management security can have effects on application security and vice-versa as they are integrated into each other.
- **Reduced Transparency**: There is very less transparency as the application is integrated to the external services. For example, the customer does not have full knowledge of the set of security measures for external PaaS service integrated with the customer's application.

Implementations

The issue of application security at the enterprise level can be addressed by the security team using a risk-based approach. It means that the team must prioritize assets, focus on identifying areas of highest risk,

and mitigate the risk. Application security at the enterprise level does not mean only to scan the vulnerabilities in the application. It goes beyond that because organizations can have thousands of applications that serve different purposes. To tackle application security, IBM came up with ASoC (Application Security on Cloud) that enables security teams to build an inventory of their application assets, classify and prioritize their assets by business impact before they even start security testing. Using ASoC, security team will be able to prioritize major vulnerabilities and try to remediate it that have bigger impacts on the organization. ASoC can be used to secure mobile, web and desktop applications. IBM also provides application security to domains apart from cloud.

Risk Associated with noncompliance

One of the major credit reporting agencies, Equifax, had a breach on July 2017 and attackers gained company data that consisted sensitive information of 143 million Americans including social security numbers and driver's license numbers. In addition to that, they gained names, birth dates and addresses. Around 209,000 credit card numbers were stolen while documents with personal information used in disputes for 182,000 people were also taken. Attackers were able to gain data due to a known vulnerability in the Strut 2 framework which was not patched in a timely manner. By taking advantage of the Strut 2 framework vulnerability, attackers gained access to the database and stole all the sensitive information from it. It could have been avoided by patching the software, but most importantly, they could have isolated the attack using the micro services architecture which would have helped to minimize the application security breach.

DOMAIN 11: Data Security and Encryption

Introduction

Data Security is protecting of data that are stored in various storage devices from unwanted actions of unauthorized users such as cyberattack or a data breach. Many organizations tend to avoid public cloud services to store their data because they feel they are insecure. In addition, some organizations encrypt everything in SaaS because they do not trust the provider. In that case, they should not store the data in public cloud in the first place. It is reasonable to store the data in cloud because they use cutting edge data security technologies to secure it and organizations do not need to worry about encrypting their own data. Also, cloud providers usually charge very low for data security which meets the customer's goal of spending economically. Therefore, data Security is crucial for the cloud providers as it helps them to retain the trust of their customers. Two of the essential components of data security is encryption which is useful for data confidentiality and access controls. Encryption is a process that takes legible data as input and transforms it into an output that reveals little or no information about the plain text. Access Control is a security technique that can be used to regulate who or what can view or use resources in a cloud computing environment.

Importance

Data security is achieved in cloud using following technologies:

- **Cloud data access control**: Access control should at least be implemented with a minimum of three layers i.e management plane, public and internal sharing controls, and application level controls. Management plane is the control for managing access of users that directly access the cloud platform's services. For example, logging into web console of an IaaS that allows access to data in object storage. To tackle it, most cloud platforms start with default deny access control

policies. If data is shared externally to public or partners that do not have access to the cloud platform, there will be a second layer of controls for this access.

- **Data (At-Rest) Encryption**: Cloud providers encrypt the data on various levels which makes it difficult for the hackers to attack and, therefore, secures the customers data. IaaS volumes can be encrypted using different methods, depending on the data. Volume storage can be encrypted using instance managed encryption and externally managed encryption. Object and file storage can be encrypted using client-side encryption, server-side encryption, and proxy encryption. PaaS providers provide application layer encryption and database encryption. SaaS customers are provided with provider-managed encryption and proxy encryption.

Challenges

- Different systems and datasets may have widely differing classifications and sensitivity levels. To ensure the proper security policy is applied to sensitive data, systems, and applications that store or process this data are often kept physically separate from others. However, in a multi-tenant environment such as the cloud, this may not be feasible. In addition, ensuring internal policies related to data handling and access control may be difficult when migrating systems and applications to a cloud provider. This can be a problem when integrating public cloud services to an existing private cloud (a hybrid cloud scenario), as well as during a wholesale migration of data and systems to a public cloud environment.
- It can be very challenging to implement encryption internally due to key management and maintenance, performance issues, and access controls. Extending internal encryption platforms and capabilities into the cloud can seem daunting at best. For example, how will administrators manage encryption keys for data and systems in the cloud? When encryption keys need to be generated or revoked, how can this easily be accomplished for resources hosted elsewhere? Will cloud service providers (CSPs) need access to keys, and what kinds of risk will this introduce? For hybrid clouds, handling encryption may be less of an issue, but moving to a public cloud may pose significant challenges.

Implementations

Google cloud platform provides encryption At-Rest using several layers of encryption to protect data. Either distributed file system encryption or database and file storage encryption is in place for almost all files; and storage device encryption is in place for almost all files.
Each data chunk is encrypted at the storage level with an individual encryption key. Two chunks will not have the same encryption key even if they are part of the same Google cloud storage object, owned by the same customer, or stored on the same machine. Google platform encrypts customer content stored at rest, without any action from the customer, using one or more encryption mechanisms, except for some minor exceptions like temporary files used by storage systems. The key used to encrypt the data in a chunk is called a data encryption key (DEK). The DEKs are encrypted with a key encryption key (KEK). KEKs are stored centrally in Google's key management service (KMS), a repository built specifically for this purpose. KEKs are exportable from KMS by design. All encryption and decryption with these keys must be done within KMS. This helps prevent leaks and misuse. Google's root of trust, the root KMS master key, is kept in RAM and is also secured in physical safes in limited Google locations in case of a global restart.

Risk Associated with noncompliance

Yahoo data breach: In September 2016, Yahoo, while in the negotiations with Verizon to sell the company announced that they had the biggest data breach in 2014 which is the biggest breach in history.

Due to the attack, hackers obtained names, email addresses, date of birth, and telephone of 500 million users. Later that year, they revealed that they had another data breach in 2013 by different group of hackers. Along with information that was obtained in 2014, these hackers also obtained security questions and answers of yahoo users. Around 3 billion accounts were hacked due to the data breach of 2013. Due to these data breaches, Verizon paid only 4.48 billion dollars to buy the company which was valued at around 100 billion dollars once. Therefore, data breach like the one that happened with Yahoo can cause the customers to lose trust in the cloud providers causing the providers to lose revenue and losing millions of dollars in compensation.

DOMAIN 12: Identity, Entitlement and Access Management

Introduction

Identity, Entitlement and Access Management (IAM) has been greatly affected by cloud computing. Cloud computing introduces multiple changes to how IAM was traditionally managed for internal systems. The most important difference is the relationship between the cloud provider and the cloud user. IAM cannot be managed by only one of them and thus a trust relationship, designation of responsibilities and technical mechanics to enable them are required. IAM standards followed by the cloud providers are Security Assertion Markup Language (SAML) 2.0, OAuth, OpenID, eXtensible Access Control Markup Language (XACML), and System for Cross-domain Identity Management (SCIM).

The 'identity' part of identity management focuses on the processes and technologies for registering, provisioning, propagating, managing, and deprovisioning identities. Most cloud providers turn to federation for identity management. When using federation, the cloud user needs to determine the authoritative source that holds the unique identities they will federate. In addition to that, Multifactor Authentication (MFA) is provided by the cloud providers for authentication.

An Entitlement is used for mapping identities to authorizations and any required attributes. For example, a user can access a resource when given attributes have designated values.

An access control allows or denies the expression of the authorization, so it includes aspects like assuring that the user is authenticated before allowing access.

Importance

IAM has gained a lot of importance due to the following reasons:

- **User Experience Enhancement**: Using SSO, it has helped to eliminate the need for users to remember and input multiple passwords to access different areas of your system.
- **Security Profile Enhancement**: Along with SSO, IAM provides SAML 2.0 that can help to authenticate and authorize users based on the access level indicated in their directory profiles.
- **Reduced IT costs**: As the tasks of managing the identity management falls in the hands of the cloud provider, organizations do not need to invest on IT desk jobs that handle user management issues.

Challenges

- **2-factor authentication to prevent a security breach**: If an organization is using a lot of cloud applications and they are worried about a security breach, they would be looking for a two-factor authentication but there are too many applications to protect and on top of that employees need to

access the network remotely. In addition to that, if the single sign-on solution does not have a 2-factor system, they will have to use a third-party vendor and integrate which will be costly for the organization.

- **Usability issues due to multiple levels of security**: An organization wants to implement all the security like encryption, 2-factor, single sign-on but they would have to make sure that they do not bother their users if they are coming from known devices or known network. They should only challenge the users if they are accessing it from an untrusted network.

Implementations

Microsoft Azure identity and access management solutions help IT protect access to applications and resources across the corporate data center and into the cloud. This enables additional levels of validation, such as multifactor authentication and conditional access policies. Monitoring suspicious activity through advanced security reporting, auditing and alerting helps mitigate potential security issues. Microsoft Azure IAM simplifies user access to any cloud application i.e. enables single sign-on (SSO) to thousands of cloud applications across many device platforms. It protects insensitive data using Azure Multi-Factor Authentication which is provided free of cost. It helps to integrate active directory and other on-premise directories to the azure active directory. It enables to bring enterprise directory and ID management to the cloud i.e. centrally manage employee access to Microsoft Online Services and non-Microsoft cloud applications. MFA for office 365 helps to secure access to office 365, Azure active directory premium and software-as-a-service applications.

Risk Associated with noncompliance

Due to a data breach in Utah Department of Technology Services (DTS) computer server, Medicaid and CHIP claim data was acquired by the hackers. It has been estimated that 280,000 victims had their SSNs stolen and around 500, 000 other victims had less sensitive personal information stolen. Hackers were able to get the data due to an error on the server at the password authentication level. It has been said Utah DTS has security processes in place to prevent illegal server, but the hacked server was not configured according to normal procedures. There may be a possibility that default password was being used on the server. These attacks could have been avoided if they would have used IAM.

DOMAIN 13: Security as a Service

Introduction

Security as a service (SecaaS) providers offer security capabilities as a cloud service. This includes dedicated SecaaS providers, as well as packaged security features from general cloud-computing providers. SecaaS must follow the below criteria:

- SecaaS includes security products or services that are delivered as a cloud service
- The services must the meet the essential NIST characteristics – On Demand Service, Broad Network Access, Resource Pooling, Rapid Elasticity/Expansion and Measure Service, for cloud computing.

Importance

Importance of SecaaS can be measured by the following benefits it offers:

- **Cloud-computing benefits:** The normal potential benefits of cloud computing—such as reduced capital expenses, agility, redundancy, high availability, and resiliency—all apply to SecaaS. As with any other cloud provider the magnitude of these benefits depends on the pricing, execution, and capabilities of the security provider.
- **Staffing and expertise:** Many organizations struggle to employ, train, and retain security professionals across relevant domains of expertise. This can be exacerbated due to limitations of local markets, high costs for specialists, and balancing day-to-day needs with the high rate of attacker innovation. As such, SecaaS providers bring the benefit of extensive domain knowledge and research that may be unattainable for many organizations that are not solely focused on security or the specific security domain.
- **Intelligence-sharing:** SecaaS providers protect multiple clients simultaneously and have the opportunity to share data intelligence and data across them. For example, finding a malware sample in one client allows the provider to immediately add it to their defensive platform, thus, protecting all other customers. Practically speaking this isn't a magic wand, as the effectiveness will vary across categories, but since intelligence-sharing is built into the service, the potential upside is there.
- **Deployment flexibility:** SecaaS may be better positioned to support evolving workplaces and cloud migrations, since it is itself a cloud-native model delivered using broad network access and elasticity. Services can typically handle more flexible deployment models, such as supporting distributed locations without the complexity of multi-site hardware installations.
- **Insulation of clients:** In some cases, SecaaS can intercept attacks before they hit the organization directly. For example, spam filtering and cloud-based Web Application Firewalls are positioned *between* the attackers and the organization. They can absorb certain attacks before they ever reach the customer's assets.
- **Scaling and cost:** The cloud model provides the consumer with a "Pay as You Grow" model, which also helps organizations focus on their core business and lets them leave security concerns to the experts.

Challenges

Challenges are reflected in the below mentioned potential concerns with SecaaS:

- **Lack of visibility:** Since services operate at a remove from the customer, they often provide less visibility or data compared to running one's own operation.
- **Regulation differences:** Given global regulatory requirements, SecaaS providers may be unable to assure compliance in all jurisdictions that an organization operates in.
- **Handling of regulated data:** Customers will also need assurance that any regulated data potentially vacuumed up as part of routine security scanning or a security incident is handled in accordance with any compliance requirements; this also needs to comply with aforementioned international jurisdictional differences. For example, employee monitoring in Europe is more restrictive than it is in the United States, and even basic security monitoring practices could violate workers' rights in that region. Likewise, if a SecaaS provider relocates its operations, due to data center migration or load balancing, it may violate regulations that have geographical restrictions in data residence.
- **Data leakage:** As with any cloud computing service or product, there is always the concern of data from one cloud user leaking to another. This risk isn't unique to SecaaS, but the highly sensitive nature of security data (and other regulated data potentially exposed in security scanning or incidents) does mean that SecaaS providers should be held to the highest standards of multitenant isolation and segregation. Security-related data is also likely to be involved in litigation, law enforcement investigations, and other discovery situations. Customers want to ensure their data will not be exposed when these situations involve another client on the service.

- **Changing providers:** Although simply switching SecaaS providers may on the surface seem easier than swapping out on-premises hardware and software, organizations may be concerned about lock-in due to potentially losing access to data, including historical data needed for compliance or investigative support.
- **Migration to SecaaS:** For organizations that have existing security operations and on-premises legacy security control solutions, the migration to SecaaS and the boundary and interface between any in-house IT department and SecaaS providers must be well planned, exercised, and maintained.

Implementation

Following are some of the SecaaS offerings:

- **Identity, Entitlement, and Access Management Services:** Identity-as-a-service is a generic term that covers one or many of the services that may comprise an identity ecosystem, such as Policy Enforcement Points (PEP-as-a-service), Policy Decision Points (PDP-as-a-service), Policy Access Points (PAP-as-a-service), services that provide Entities with Identity, services that provide attributes (e.g. Multi-Factor Authentication), and services that provide reputation.
- **Cloud Access and Security Brokers (also known as Cloud Security Gateway):** These products intercept communications that are directed towards a cloud service or directly connect to the service via API in order to monitor activity, enforce policy, and detect and/or prevent security issues. They are most commonly used to manage an organization's sanctioned and unsanctioned SaaS services. While there are on-premises CASB options, it is also often offered as a cloud-hosted service.
- **Web Security:** Web Security involves real-time protection, offered either on-premises through software and/or appliance installation, or via the Cloud by proxying or redirecting web traffic to the cloud provider (or a hybrid of both). This provides an added layer of protection on top of other protection, such as anti-malware software to prevent malware from entering the enterprise via activities such as web browsing.
- **Email Security:** Email Security should provide control over inbound and outbound email, protecting the organization from risks like phishing and malicious attachments, as well as enforcing corporate policies like acceptable use and spam prevention, and providing business continuity options.
- **Web Application Firewalls:** In a cloud-based WAF, customers redirect traffic (using DNS) to a service that analyzes and filters traffic before passing it through to the destination web application. Many cloud WAFs also include anti-DDoS capabilities.

DOMAIN 14: Related Technologies

Introduction

Related technologies fall into the following categories:

- Technologies that rely exclusively on cloud computing to operate.
- Technologies that don't necessarily rely on cloud, but are commonly seen in cloud deployment.

Following technologies leverage cloud computing for their operations:

1. Big Data

Big Data includes a collection of technologies for working with extremely large datasets that traditional data processing tools are unable to manage. The 3 Vs that form the core definition of big data are:

- High Volume: a large size of data, in terms of number of records or attributes
- High Velocity: fast generation and processing of data
- High Variety: structured, semi structured or unstructured data.

Implementation

Cloud Computing, due to its elasticity and massive storage capabilities, is very often where big data projects are deployed. Big Data technologies are very commonly integrated into cloud computing applications and offered by cloud providers as IaaS or PaaS.

- **Distributed data collection:** Mechanisms to ingest large volumes of data, often of a streaming nature. This could be as "lightweight" as web-click streaming analytics and as complex as highly distributed scientific imaging or sensor data. Not all big data relies on distributed or streaming data collection, but it is a core big data technology.
- **Distributed storage:** The ability to store the large data sets in distributed file systems (such as Google File System, Hadoop Distributed File System, etc.) or databases (often NoSQL), which is often required due to the limitations of non-distributed storage technologies.
- **Distributed processing:** Tools capable of distributing processing jobs (such as map reduce, spark, etc.) for the effective analysis of data sets so massive and rapidly changing that single origin processing can't effectively handle them.

Challenges

- Big data has provided organizations with terabytes of data, it is a challenge to analyze and manage this data under traditional as well as cloud framework.
- Moving large sets of data and providing the details needed to access it, is a challenge. These large sets of data often carry sensitive information like credit/debit card numbers, addresses and other details, raising data security concerns.
- Some cloud models are still in the deployment stage and basic DBMS is not tailored for Cloud computing. Data Acts is also a serious issue which requires data centers to be closer to a user than a provider.
- Data replication must be done in a way which leaves zero room for error; otherwise it can affect the analysis stage. It is crucial to make the searching, sharing, storage, transfer, analysis, and visualization of this data as smoothly as possible.

2. Internet of Things (IoT)

IoT is a blanket term for non-traditional computing devices used in the physical world that utilize internet connectivity. IoT is generating an unprecedented amount of data, which in turn puts a tremendous strain on the internet infrastructure. As a result, companies are working to find ways to alleviate that pressure and solve the data problem. Cloud computing can be a major part by making all the connected devices work together as Cloud Computing provides a pathway for the data to travel to its destination.

Implementations

Amazon Web Services, one of several IoT cloud platforms, points out six advantages and benefits of cloud computing:

· Variable expense allows you to only pay for the computing resources you use, and not more.
· Providers such as AWS can achieve greater economies of scale, which reduce costs for customers.
· You no longer need to guess your infrastructure capacity needs.

- Cloud computing increases speed and agility in making resources available to developers.
- You can save money on operating data centers.
- You can deploy your applications worldwide in a matter of minutes.

Challenges

- Secure data collection and sanitization.
- Device registration, authentication, and authorization. One common issue encountered today is use of stored credentials to make direct API calls to the back-end cloud provider. There are known cases of attackers decompiling applications or device software and then using those credentials for malicious purposes.
- API security for connections from devices back to the cloud infrastructure. Aside from the stored credentials issue just mentioned, the APIs themselves could be decoded and used for attacks on the cloud infrastructure.
- Encrypted communications. Many current devices use weak, outdated, or non-existent encryption, which places data and the devices at risk.
- Ability to patch and update devices so they don't become a point of compromise. Currently, it is common for devices to be shipped as-is and never receive security updates for operating systems or applications. This has already caused multiple significant and highly publicized security incidents, such as massive botnet attacks based on compromised IoT devices.

Conclusion

In this paper, we covered risks associated with the security in cloud, and described the role of service providers and customers in the implementation of the security in cloud. In summation, paper demonstrates how CSA guidelines provides a roadmap to implement security while migrating from the tradition network to the cloud, and delineates the importance, challenges and risk associated in the migration.

References

1. Cloud Security Alliance, *Security Guidance for critical areas of focus in cloud computing*, Creative Commons Attribution-Noncommercial-Share Alike 4.0 International License, CC-BY-NC-SA 4.0, vol. 4, 2017
2. Amazon Web Services, *CSA Consensus Assessments Initiative Questionnaire,* 2017
3. C. Brett, *"Information Governance: 6 Cloud Risks to Expose",* Document Strategy, Found at: http://www.consultparagon.com/blog/information-governance-cloud-assessment, Nov 30, 2016
4. A. Meola, "*The roles of Cloud Computing and fog computing in the Internet of Things evolution*", Found at: http://www.businessinsider.com/internet-of-things-cloud-computing-2016-10, Dec 20, 2016
5. K. Riaz, "*Big data and Cloud Computing Challenges and Opportunities*", Found at: http://bigdata-madesimple.com/big-data-and-cloud-computing-challenges-and-opportunities/, Jun 02, 2017