Best Practices Against Cloud Security Incidents

Objectives:

At the end of this episode, I will be able to:

Understand what the best practices against Cloud Security incidents are.

Explain what the challenges in handling and responding to cloud security
incidents are.

Identify what the incident handling responsibilities in Cloud Computing are.

Define the steps necessary to eradicate Cloud Security incidents.

External Resources:

Best Practices Against Cloud Security Incidents

Incident Handling Responsibilities in Cloud -

```
    Incident Handling Responsibilities in Cloud.docx
```

Challenges in handling and responding to cloud security incidents:

Architecture and Identification -

o Deletion in the cloud:

```
• The total volume of data and users operating in a cloud ecosystem constrains
```

the amount of backups the CSP will retain.

```
• CSPs may not implement the necessary methods to retrieve deleted data in
```

IaaS or PaaS delivery models.

o Recovering overwritten data:

```
• It is very difficult to recover data marked as deleted, as it may get
```

overwritten by another user sharing the same cloud.

o Interoperability issues among CSPs:

```
• Collection and preservation of forensic evidence is challenging as there is
```

a lack of interoperability among CSPs.

o Single points of failure:

```
• The cloud ecosystem has single points of failure, which may adversely impact
```

the evidence acquisition process.

o No single point of failure for criminals:

```
• Collection and analysis of evidentiary data from distributed and disparate
```

sources is highly difficult as criminals may choose one CSP to store their
data, a second CSP to obtain computing services, and a third CSP to route all
their communications.

o Detection of the malicious act:

```
• It is tough for an incident handler to detect a malicious act by identifying
```

a series of small changes made across many systems and applications as a result
of attacks against a cloud.

o Malicious code may circumvent VM isolation methods:

```
• Vulnerabilities in server virtualization may allow malicious code to evade
```

VM isolation methods and interfere with either other guest VMs or the
hypervisor itself.

o Multiple venues and geo-locations:

```
• Managing the scope of data collection is challenging as distributed data
```

collection and chain of custody from multiple venues or geo-locations can
cause various jurisdictional issues.

o Lack of transparency:

- Operational details are not always clear enough to incident handlers, which can result in a lack of trust and difficulties with auditing.

o Cloud confiscation and resource seizure:

- Cloud confiscation and resource seizure may affect the business continuity of other tenants.

o Errors in cloud management portal configurations:

- Configuration errors in cloud management portals may allow an attacker to gain control, reconfigure, or delete another cloud customer’s resources or applications.
- It is hard to find the source of such unauthorized change as the cloud management portal is being used by multiple tenants simultaneously.

o Potential evidence segregation:

- Segregation of potential evidence pertaining to one tenant in a multi-tenant cloud system is a challenge without breaching the confidentiality of other tenants.

o Secure provenance / Data chain of custody:

- It is a challenge for incident handlers to maintain proper chain of custody and security of data, metadata, and possibly hardware, as determining ownership, custody, or exact location may be difficult.

Data Collection -

o Decreased access and data control:

- In every combination of cloud service model and deployment model, the incident handler faces the challenge of limited access and control to the forensic data.
- CSPs hide data locations to ease data movement and replication.

o Data location:

- Collecting data is challenging because of the flexibility CSPs have to migrate data between data centers and geographic regions.

o Imaging and isolating data:

- Imaging and isolating a migrating data target is challenging in the cloud ecosystem due to its key characteristics: elasticity, automatic provisioning/deprovisioning of resources, redundancy, and multi-tenancy.

o Data available for a limited time:

- Data collection and preservation of VM instances is challenging due to the lack of standard practices and tools.

o Live forensics:

- Validating the integrity of data collected is challenging as data within the cloud is volatile and frequently changing. Also, live forensics tools may make modifications to the suspect system.

o Resource abstraction:

- Identifying and collecting evidentiary data is challenging because resources are abstracted and the information about cloud architecture, hardware, hypervisors, and file system types is not always readily available to help us to understand the cloud environment.

o Additional collection is often infeasible in the cloud:

- Collecting additional evidence is often unfeasible in the cloud as specific

data locations are not known, the sizes may be huge, and non-standard protocols
and mechanisms may be used to exchange data and poorly or not documented.

o Ambiguous trust boundaries:

```
• Not all CSPs implement vertical isolation for tenants’ data that can lead to
```

questionable data integrity.

o Data integrity and evidence preservation:

```
• For stakeholders, maintaining evidence quality, evidence admissibility,
```

data integrity, and evidence preservation is challenging as faults and
failures in data integrity are shared among multiple actors, and the chance
for such faults and failures is higher in the cloud environment due to sharing
of data/responsibilities.

Analysis -

o Evidence correlation:

```
• Correlation of an activity across multiple CSPs is a challenge due to the
```

lack of interoperability.

o Timestamp synchronization:

```
• Correlating the activities observed with accurate time synchronization is a
```

challenge as the timestamps may be inconsistent between different sources.

o Use of metadata:

```
• Using metadata as an authentication method may be at risk, as common fields
```

(creation date, last accessed date, last modified date) may change when data
is moved into and within the cloud and at the time of data gathering process.

```
• Check to see if the CSP preserves metadata and if it is readily accessible
```

for e-discovery purposes.

Legal -

o Missing terms in contract or SLA:

```
• Lack of forensic related terms in the cloud contracts is challenging as it
```

could prevent the generation and collection of existing appropriate data as
well as generating potentially appropriate data.

o Limited investigative power:

```
• In civil cases, incident handlers are often provided with limited
```

investigative power to properly obtain data under the respective jurisdictions.

o Reliance on cloud providers:

```
• Acquiring forensic data from cloud is challenging as it requires CSPs
```

cooperation, which may be limited by the number of employees and other
resources at the provider end.

o Physical data location:

```
• Specifying the physical location(s) of data on a subpoena is challenging as
```

the requestor often does not know where the data is stored physically.

o Lack of international agreements and laws:

```
• Gaining access to and exchanging data is challenging due to the lack of
```

international collaboration and legislative mechanisms.

How do we eradicate Cloud Security incidents? -

Eradication is the process of removing the compromised cloud networks and
applications that can represent attacks.

```
• Clean up the infected software
• Rebuild or reconstruct compromised networks
• Notify the relevant officials about the incident
```