Handling Email Security Incidents

Objectives:

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

Understand what the best practices against email security incidents are.

Explain what the challenges in handling email security incidents are.

Identify what the incident handling responsibilities for email security incidents are.

Define the steps necessary to contain, eradicate, and recover from email security incidents.

External Resources:

Handling Email Security Incidents

Email attacks can cause leakage of sensitive data, installation of malware, or other malicious activities that can inflict huge financial and resource losses to the organization.

We can categorize email crime in two ways:

• Crimes Committed by Sending Emails - Some of the attacks that fall under this category are:

```
o Spamming
o Phishing
o Mail bombing
o Mail storms
o Malware distribution
```

• Crimes Supported by Emails - Some of the attacks that fall under this category are:

```
o Identity theft
o Cyberstalking
o Child pornography
o Abduction
```

What are the different types of phishing? -

```
Spear Phishing - targeted phishing attack aimed at specific individuals within
an organization

Whaling - attacker targets high profile executives like CEO, CFO, politicians,
and celebrities who have access to confidential and highly valuable information

Pharming - redirects web traffic to a fraudulent website by installing a
malicious program on the target device(s); Pharming attacks are also known as
"Phishing without a Lure," which is performed either by using DNS Cache
Poisoning or Host File Modification

Spimming - exploits instant messaging platforms to flood spam across the networks

Puddle Phishing - attack aimed at small organizations

CEO Scam - attacker spoofs email address of the CEO and uses it to send
request to share a report or conduct a wire transfer to employees responsible
such as the HR and finance department
```

How do we Prepare for Handling Email Security Incidents? -

```
▪ Email filtering
▪ Email monitoring
▪ Establish independent communication channels
▪ Training and awareness for employees
▪ Acceptable usage policy
▪ Local archives or backups
```

How do we detect and contain Email Security Incidents? -

Incident responders can detect and verify if the email is malicious by looking for the following:

```
▪ Unexpected attachments from unknown users, clients, vendors, or peers
▪ Attachments with unusual or unrecognized formats
▪ Difference in the email ID of the sender and display name
▪ Emails from IDs that do have incomplete or incorrect organization name or
use numbers in place of letters in the name
▪ Emails with links, which display a different website or URL when hovered on
or have URL with incorrect name or domain
▪ Obvious misspellings and strange use of punctuation
▪ Emails that do not have a complete signature and contact details of the sender
```

What about Analyzing Email Headers? -

The following information can be gathered via E-mail Header Analysis:

```
▪ Return Path
▪ Recipient's e-mail address
▪ Name of the e-mail server
▪ Type of sending service
▪ IP Address of the sending server
▪ Unique message number
▪ Date and time e-mail was sent
▪ Attachment(s) information
▪ Sender Policy Frameowrk (SPF)
▪ DomainKeys Identified Mail (DKIM)
```

SPF is an email validation protocol used by domain owners for preventing spoofing of emails; Incident responders can analyze the authenticity of the sender using the SPF results:

```
▪ None - no SPF record was found

▪ Pass - SPF record exits and IP address is authorized; includes a plus (+)
sign in front of the IP address

▪ Neutral - means that the domain owner does not want to disclose the specific
IP address authorized in SPF record

▪ Fail - IP address is not authorized to send email for this domain; shown by
a -all command in the record

▪ SoftFail - between neutral and fail; means that the mail is authorized but
is tagged as suspicious or spam

▪ TempError - temporary error such as a technical issue during verification

▪ PermError - SPF record cannot be verified due to syntax or format errors in
the record
```

DomainKeys Identified Mail (DKIM) - an email authentication standard designed to detect spoofing

A domain owner can encrypt the domain's outgoing mail headers and add a digital signature to the outgoing emails for better authentication.

DKIM will display the following results:

```
Pass - e-mail is signed and the signature passes the verification tests

Neutral - e-mail is signed but the signature has syntax errors, so it cannot
be processed

Fail - e-mail is signed but the signature does not pass the verification tests

Policy - e-mail is signed but some part of the signature is not acceptable by
the administrative management domains (ADMD)

TempError - e-mail is not verified due to temporary errors, such as "cannot
retrieve public key"

PermError - e-mail is not verified due to permanent errors, such as the
absence of required header field information
```

Steps to Analyze E-mail in Gmail -

```
1. Open an email you want to analyze
2. Click the "More" option (three vertical dots) from the top-right of the message
3. From the drop-down menu, click "Show original" option
4. The mail will open a new tab displaying the original message
5. Check for the SPF and DKIM credentials of the email to verify its authenticity
```

Steps to Analyze E-mail in Yahoo Mail -

```
1. Open an email you want to analyze
2. Click the "More" option (three horizontal dots) from the top of the message
3. From the drop-down menu, click "View raw message" option to see the complete
message source
4. Check for the SPF and DKIM credentials of the email to verify its authenticity
```

How do we examine the Originating IP Address? -

In the process of detecting and containing malicious emails, incident responders should examine the originating IP address of the emails.

The following steps are involved in the process of examining the originating IP address:

```
1. Open the email to trace and find its header
2. Collect the IP address of the sender from the header of the received mail
3. Search for the IP in the WHOIS database
4. Look for the geographic address of the sender in the WHOIS database
```

What can logs tell us? -

Examining Microsoft Exchange Email Server Logs -

Microsoft Exchange uses the Microsoft Extensible Storage Engine (ESE) which in turn employs Messaging Application Programming Interface (MAPI) for the collaboration of various email applications in the organization.

Incident handlers should primarily focus on the following files:

```
▪ .edb database files (responsible for MAPI information)
▪ .stm database files (responsible for non-MAPI information)
▪ checkpoint files
▪ temporary files
```

The Performance Analysis of Logs (PAL) Tool (https://github.com) can be used to monitor and analyze the logs for identifying phishing and malware distribution emails.

The Get-MessageTrackingLog PowerShell command can be used to trace the flow of email from sender to receiver.

Examining Linux Email Server Logs -

Sendmail is the command used to send emails via Linux or UNIX systems.

It requires the information regarding the source and destination addresses, the sender and recipient addresses, and the email message ID.

Sendmail uses Syslog to maintain logs on the system.

The syslog configuration file, /etc/syslog.conf determines the location of these syslog service logs.

The syslog configuration file contains information on the logging priority, where logs are sent, and what other actions may be taken.

The syslog.conf also provides the location of the log file for email, which is usually /var/log/mailog.

The /var/log/mailog file contains source and destination IP addresses, date and time stamps, and other information necessary to validate the data within an email header.

Examining Novell GroupWise Email Server Logs -

Stores the user's messages in almost 25 proprietary databases. It stores all the databases in the OFUSER Directory object and references them by username, followed by a unique ID and the .db extension.

The NGWDFR.DB database, present in the OFMSG directory object, is used for delayed or deferred emails.

Guardian (Ngwguard.db) is a specialized database that:

```
▪ Maintains centralized control of the email services
▪ Tracks changes in the GroupWise environment
▪ Includes built-in safeguards like Ngwguard.fbk, Ngwguard.rfl, and Ngwguard.db,
which help in preventing data loss
```

GroupWise generates log files (.log extension) maintained in GroupWise folders, which responders can use to match an email header with a suspect's IP address. Incident responders must analyze these logs to find the anomalous emails.