Cyber Incident Playbook

Document Information

Version:	0.5
Datum:	14. Sep. 2020
Status:	Draft
Author:	Samuel Mühlebach, CISO Fides Treasury Services AG
Classification:	Intern

Content

1 Goals

In the event of a cyber incident, it is important that the organization is able to respond adequately and in a timely manner to limit the impact and restore normal operation as soon as possible.

The goal of the cyber incident playbook is to describe some cyber incident scenarios and how the organization should respond. The playbook provides incident managers and stakeholders with a consistent approach and the specific actions that may be required. Also, the playbook can be used for training and testing purposes.

This playbook should be used together with the incident response handbook which describes the incident management organization with roles and responsibilities and the incident response process.

2 Scope

A selection of cyber incidents which are relevant for Fides Treasury Services AG.

As a starting point the following three scenarios are used:

- Phishing attack
- Ransomware attack
- Distributed denial of service (DDoS) attack

3 Approach

The description of the cyber incident scenarios is along the incident response management phases: preparation, detection, analysis, remediation, and post incident.

For each phase, first the objective is stated and then the activities with a description how the organization should respond including the responsibilities.

4 Phishing Attack

Phishing is the act of attempting to acquire information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. Spear Phishing is where an attacker uses information about employees and the company to make the Phishing campaign more persuasive and realistic.

4.1 Preparation

The preparation phase has the following objectives:

- Prepare the organization to respond to a cyber incident in a timely and effective manner
- Inform employees of their role in remediating a phishing incident, including reporting mechanisms

Activity	Description	Stakeholders
Threat intelligence	Review threat intelligence for phishing threats to the organization, as well as common patterns and newly developing risks and vulnerabilities.	CISO
	Review recent phishing attack incidents	CISO
	Define key risk indicators (KRI) for phishing attacks and alerts for the security information and event management (SIEM) solution.	CISO
Control effectiveness	Verify effectiveness of security controls to prevent from phishing attacks	CISO
Awareness	Conduct regular awareness campaigns to highlight the risk to be a victim of a cyber attack (e.g. phishing, ransomware, social engineering).	CISO
Training	Ensure that regular security training is mandated for all employees.	CISO

Table 1: Preparation

4.2 Detection

The detection phase has the following objectives:

- Detect and confirm the phishing attack
- Open a case
- Inform IT incident response management
- Classify the incident

Activity	Description	Stakeholders
Detect phishing attack	Monitor email communication channels for phishing attacks.	SOC CSIRT
	Notifications by internal users of suspicious emails.	IT Service Desk
Confirm phishing attack	Verify reported phishing attack and confirm or deny.	IT Service Desk
Open case	Open a ticket in the incident response journal.	IT Service Desk
Notify IT incident response manager	Inform the IT incident manager and hand-over the case.	IT Service Desk
Classify incident	Classify the incident according the classification matrix outlined in the incident response management handbook.	IT Incident Response Manager

Table 2: Detection

4.3 Analysis

The analysis phase has the following objectives:

- Mobilize CSIRT
- Perform initial investigations
- Secure evidence
- Call external experts if needed
- Determine business impact
- Report incident
- Inform about status and progress

Activity	Description	Stakeholders
Mobilize CSIRT	Mobilize CSIRT	IT Incident Response Manager

Activity	Description	Stakeholders
Initial investigation of the incident	Collate initial incident data ▪ Identify the phishing email ▪ How did the phishing email reach the organization? ▪ How many users have received the phishing email? ▪ Has any user clicked on the phishing link or opened the attachment? ▪ Has the phishing email caused any damage? ▪ Why has the phishing email not been detected and blocked by the malicious code prevention?	CSIRT
Secure evidence	Secure evidence such as original emails, attachments, email logs, AV logs, proxy logs, etc. for further investigations, including copies of suspected malicious software and forensic copies of affected system(s) for future analysis and as chain of custody.	CSIRT
External support	Call external experts if needed	IT Incident Response Manager
Business impact	▪ Identify any data, systems, or services that have been affected ▪ Identify user credentials compromised or at risk ▪ Identify business impacts of the attack (e.g. client data, financial loss, reputation damage) ▪ Identify how widespread the attack is across the organization	IT Incident Response Manager CSIRT
Report incident	Inform management and stakeholders about the incident and the findings of the initial analysis. Distinguish between confirmed facts and preliminary findings which are still under investigations.	IT Incident Response Manager
Inform about status and progress	Inform affected users, system managers, and responsible business managers. Continuously update status and progress of the incident.	IT Incident Response Manager

Table 3: Analysis

4.4 Remediation – Contain, Eradicate and Recover

The analysis phase has the following objectives:

- Limit the damage
- Emergency operation
- Return to normal operation

Activity	Description	Stakeholders
Containment and eradication	▪ Scan the whole environment for the phishing email and its payload (malicious attachments) ▪ Remove phishing emails from inboxes and/or quarantine ▪ Block email address(es) of phishing email sender ▪ Block URLs to prevent communication with command and control servers of the attacker	CSIRT SOC
Recovery	▪ Complete vulnerability scanning of all systems ▪ Deploy any necessary patches ▪ Re-set the credentials of all involved users accounts and systems accounts ▪ Restart compromised systems and suspended services ▪ Restore any corrupted or destroyed data ▪ Establish monitoring to detect further suspicious activity	CSIRT SOC
Inform about status and progress	Continuously update status and progress of the incident until incident is closed and normal operation has been restored.	IT Incident Response Manager
Report incident	Inform management and stakeholders about the successful restoration of normal operation, business impact, and further actions needed if so (e.g. information of audit and risk committee, clients, and/or regulator.	IT Incident Response Manager

Table 4: Remediation

4.5 Post Incident

The analysis phase has the following objectives:

- Complete an incident report including all incident details and activities

- Complete lessons learned for continuous improvement of the incident response management
- Publish appropriate internal and external communications

Activity	Description	Stakeholders
Incident report	▪ Create a post-incident report that includes: ▪ Chronological order of all actions taken ▪ Business impact (client data, personal data, secret business information, financial loss, reputation damage, violation of regulator or legal requirements) ▪ Evidence found and secured ▪ Root cause and circumstances responsible for the incident ▪ Lessons learned (what went well and what should be improved)	IT Incident Response Manager
Awareness	▪ Consider to use the incident as an opportunity to reinforce the phishing awareness message.	CISO

Table 5: Post incident

5 Ransomware Attack

Ransomware is a type of malicious software in which the data on a victim's computer is locked by encryption, and payment is demanded before the ransomed data is decrypted and access is returned to the victim. The motive for ransomware attacks is in most case monetary. The victim is usually notified by the attackers with instructions about the payment.

5.1 Preparation

The preparation phase has the following objectives:

- Prepare to respond to cyber incident in a timely and effective manner
- Inform employees of their role in remediating a ransomware incident including reporting mechanisms

Activity	Description	Stakeholders
Threat intelligence	Review threat intelligence for ransomware threats to the organization, as well as common patterns and newly developing risks and vulnerabilities.	CISO
	Review recent ransomware attack incidents	CISO
	Define key risk indicators (KRI) for ransomware attacks and alerts for the security information and event management (SIEM) solution.	CISO
Control effectiveness	Verify effectiveness of security controls to prevent from ransomware attacks	CISO
Awareness	Conduct regular awareness campaigns to highlight the risk to be a victim of a cyber attack (e.g. phishing, ransomware, social engineering).	CISO
Training	Ensure that regular security training is mandated for all employees.	CISO

Table 6: Preparation

5.2 Detection

The detection phase has the following objectives:

- Detect and confirm the ransomware attack
- Open a case
- Inform IT incident response management
- Classify the incident

Activity	Description	Stakeholders
Detect ransomware attack	Monitor alerts from malicious code prevention and endpoint security for ransomware attacks.	SOC CSIRT
	Notifications by internal users of events which might be a ransomware attack.	IT Service Desk
Confirm ransomware attack	Verify reported ransomware attack and confirm or deny.	IT Service Desk
Open case	Open a ticket in the incident response journal.	IT Service Desk
Notify IT incident response manager	Inform the IT incident manager and hand-over the case.	IT Service Desk
Classify incident	Classify the incident according the classification matrix outlined in the incident response management handbook.	IT Incident Response Manager

Table 7: Detection

5.3 Analysis

The analysis phase has the following objectives:

- Mobilize CSIRT
- Perform initial investigations
- Secure evidence
- Call external experts if needed
- Determine business impact
- Report incident
- Inform about status and progress

Activity	Description	Stakeholders
Mobilize CSIRT	Mobilize CSIRT	IT Incident Response Manager

Activity	Description	Stakeholders
Initial investigation of the incident	Collate initial incident data ▪ Identify the ransomware ▪ How did the ransomware reach the organization? ▪ How many users have been affected by the ransomware attack? ▪ Which data has been encrypted by the ransomware? ▪ Why has the ransomware not been detected and blocked by the malicious code prevention?	CSIRT
Secure evidence	Secure evidence such as original emails, attachments, email logs, AV logs, proxy logs, etc. for further investigations, including copies of suspected malicious software and forensic copies of affected system(s) for future analysis and as chain of custody.	CSIRT
External support	Call external experts if needed	IT Incident Response Manager
Business impact	▪ Identify any data, systems, or services that have been affected ▪ Identify business impacts of the attack (e.g. client data, financial loss, reputation damage) ▪ Identify how widespread the attack is across the organization ▪ Decide whether BCM process should be initiated as temporary workaround	IT Incident Response Manager CSIRT
Report incident	Inform management and stakeholders about the incident and the findings of the initial analysis. Distinguish between confirmed facts and preliminary findings which are still under investigations.	IT Incident Response Manager
Inform about status and progress	Inform affected users, system managers, and responsible business managers. Continuously update status and progress of the incident.	IT Incident Response Manager

Table 8: Analysis

5.4 Remediation – Contain, Eradicate and Recover

The analysis phase has the following objectives:

- Limit the damage
- Emergency operation
- Return to normal operation

Activity	Description	Stakeholders
Containment and eradication	▪ Scan the whole environment for the ransomware ▪ Remove ransomware ▪ Block distribution channels of ransomware	CSIRT SOC
Recovery	▪ Restore data from backup ▪ Verify completeness and correctness of restored data ▪ Conduct reconciliation to ensure records with business data (e.g. transactions) are in agreement ▪ Establish monitoring to detect further suspicious activity	CSIRT SOC
Inform about status and progress	Continuously update status and progress of the incident until incident is closed and normal operation has been restored.	IT Incident Response Manager
Report incident	Inform management and stakeholders about the successful restoration of normal operation, business impact, and further actions needed if so (e.g. information of audit and risk committee, clients, and/or regulator.	IT Incident Response Manager

Table 9: Remediation

5.5 Post Incident

The analysis phase has the following objectives:

- Complete an incident report including all incident details and activities
- Complete lessons learned for continuous improvement of the incident response management
- Publish appropriate internal and external communications

Activity	Description	Stakeholders
Incident report	▪ Create a post-incident report that includes: ▪ Chronological order of all actions taken ▪ Business impact (client data, personal data, secret business information, financial loss, reputation damage, violation of regulator or legal requirements) ▪ Evidence found and secured ▪ Root cause and circumstances responsible for the incident ▪ Lessons learned (what went well and what should be improved)	IT Incident Response Manager
Awareness	▪ Consider to use the incident as an opportunity to reinforce the ransomware awareness message.	CISO

Table 10: Post incident

6 DDoS Attack

A distributed denial of service (DDoS) attack is a cyber attack in which the attacker floods the a system with a huge number of requests to disrupt the service for its intended users and legitimate requests.

6.1 Preparation

The preparation phase has the following objectives:

- Prepare to respond to cyber incident in a timely and effective manner
- Inform employees of their role in remediating a DDoS incident including reporting mechanisms

Activity	Description	Stakeholders
Threat intelligence	Review threat intelligence for DDoS threats to the organization, as well as common patterns and newly developing risks and vulnerabilities.	CISO
	Review recent DDoS attack incidents.	CISO
	Define key risk indicators (KRI) for DDoS attacks and alerts for the security information and event management (SIEM) solution.	CISO
Control effectiveness	Verify effectiveness of security controls to prevent from ransomware attacks	CISO
Awareness	Conduct regular awareness campaigns to highlight the risk to be a victim of a cyber attack (e.g. phishing, ransomware, social engineering).	CISO
Training	Ensure that regular security training is mandated for all employees.	CISO

Table 11: Preparation

6.2 Detection

The detection phase has the following objectives:

- Detect and confirm the DDoS attack
- Open a case
- Inform IT incident response management
- Classify the incident

Activity	Description	Stakeholders
Detect ransomware attack	Monitor alerts from intrusion detection system (IDS), network devices, load balancers, SOC alerts, notifications from network providers, service monitoring, and customer feedback for DDoS attacks.	SOC CSIRT
	Notifications by internal users of events which might be a DDoS attack.	IT Service Desk
Confirm ransomware attack	Verify reported DDoS attack and confirm or deny.	IT Service Desk
Open case	Open a ticket in the incident response journal.	IT Service Desk
Notify IT incident response manager	Inform the IT incident manager and hand-over the case.	IT Service Desk
Classify incident	Classify the incident according the classification matrix outlined in the incident response management handbook.	IT Incident Response Manager

Table 12: Detection

6.3 Analysis

The analysis phase has the following objectives:

- Mobilize CSIRT
- Perform initial investigations
- Secure evidence
- Call external experts if needed
- Determine business impact
- Report incident
- Inform about status and progress

Activity	Description	Stakeholders
Mobilize CSIRT	Mobilize CSIRT	IT Incident Response Manager

Activity	Description	Stakeholders
Initial investigation of the incident	Collate initial incident data ▪ Which systems and services are affected by the DDoS attack? ▪ Get in contact with network provider to determine type of DDoS attack and analysis protective measures (e.g. filtering, blocking or redirection of network traffic).	CSIRT SOC Network Provider
Secure evidence	Secure evidence such as network logs, proxy logs, etc. for further investigations.	CSIRT
External support	Call external experts if needed	IT Incident Response Manager
Business impact	▪ Identify any systems or services that have been affected ▪ Identify business impacts of the attack (e.g. business disruption, financial loss, reputation damage) ▪ Decide whether BCM process should be initiated as temporary workaround	IT Incident Response Manager CSIRT
Report incident	Inform management and stakeholders about the incident and the findings of the initial analysis. Distinguish between confirmed facts and preliminary findings which are still under investigations.	IT Incident Response Manager
Inform about status and progress	Inform affected users, system managers, and responsible business managers. Continuously update status and progress of the incident.	IT Incident Response Manager

Table 13: Analysis

6.4 Remediation – Contain, Eradicate and Recover

The analysis phase has the following objectives:

- Limit the damage
- Emergency operation
- Return to normal operation

Activity	Description	Stakeholders
Containment and eradication	▪ Activate DDoS protection measures ▪ Monitor effectiveness of DDoS protection measures and impact on systems and services.	CSIRT SOC Network Provider
Recovery	▪ Conduct reconciliation to ensure records with business data (e.g. transactions) are in agreement ▪ Establish monitoring to detect further suspicious activity	CSIRT SOC
Inform about status and progress	Continuously update status and progress of the incident until incident is closed and normal operation has been restored.	IT Incident Response Manager
Report incident	Inform management and stakeholders about the successful restoration of normal operation, business impact, and further actions needed if so (e.g. information of audit and risk committee, clients, and/or regulator.	IT Incident Response Manager

Table 14: Remediation

6.5 Post Incident

The analysis phase has the following objectives:

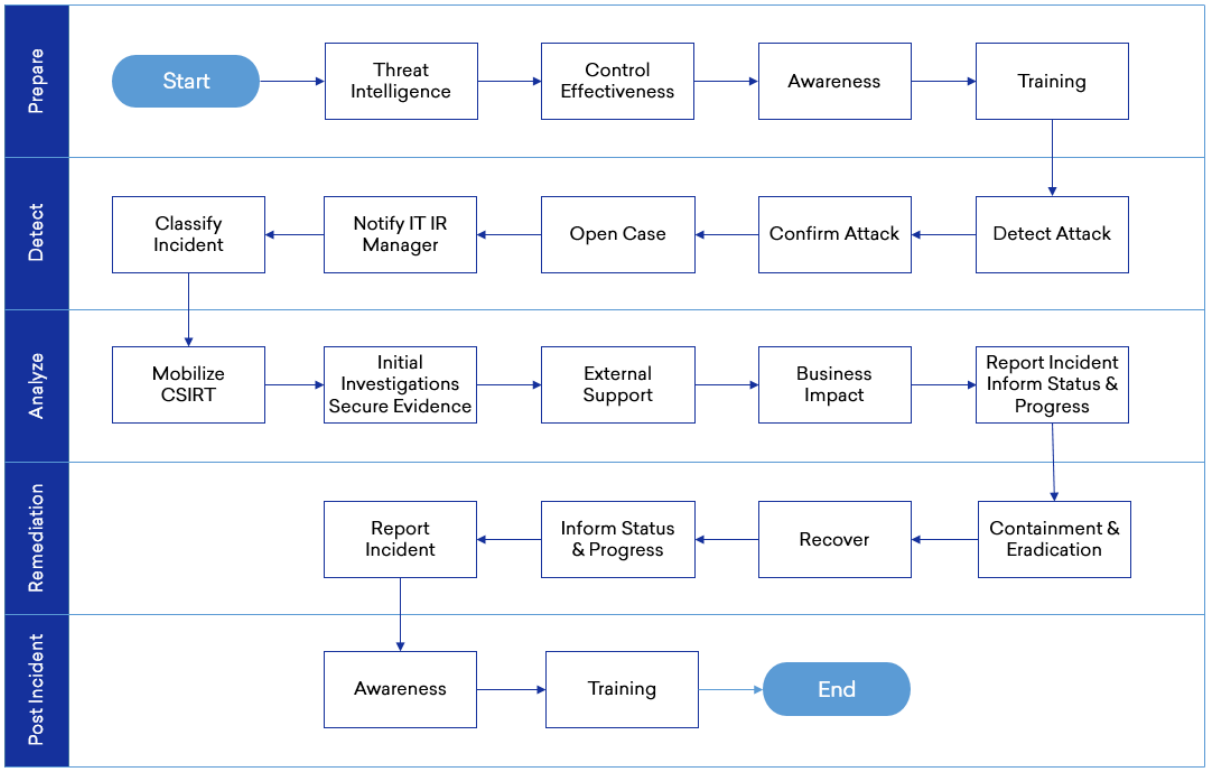
- Complete an incident report including all incident details and activities
- Complete lessons learned for continuous improvement of the incident response management
- Publish appropriate internal and external communications

Activity	Description	Stakeholders
Incident report	▪ Create a post-incident report that includes: ▪ Chronological order of all actions taken ▪ Business impact (client data, personal data, secret business information, financial loss, reputation damage, violation of regulator or legal requirements) ▪ Evidence found and secured ▪ Root cause and circumstances responsible for the incident ▪ Lessons learned (what went well and what should be improved)	IT Incident Response Manager

Activity	Description	Stakeholders
Awareness	▪ Consider to use the incident as an opportunity to reinforce the phishing awareness message.	CISO

Table 15: Post incident

7 Process Flow Diagram



8 Glossary

Tem	Description
BCM	Business Continuity Management
CISO	Chief Information Security Officer
CSIRT	Computer Security Incident Response Team
SOC	Security Operations Center

Table 16: Glossary