INCIDENT RESPONSE METHODOLOGY

IRM #19 THIRD-PARTY COMPROMISE

Guidelines to handle and respond to a third-party compromise

IRM Author: CERT SG
Contributor: CERT aDvens
IRM version: 1.0
E-Mail: cert.sg@socgen.com
Web: https://cert.societegenerale.com
Twitter: @CertSG

ABSTRACT

This Incident Response Methodology is a cheat sheet dedicated to handlers investigating on a precise security issue.

WHO SHOULD USE IRM SHEETS?

- Administrators
- Security Operation Center
- CISOs and deputies
- CERTs (Computer Emergency Response Team)

Remember: If you face an incident, follow IRM, take notes. Keep calm and contact your business line's Incident Response team or CERT immediately if needed.

→ IRM CERT SG: https://github.com/certsocietegenerale/IRM

IRM's Objective: The objective of this Incident Response Methodology (IRM19) is to provide guidance on managing and responding to incidents involving the compromise of a third-party with which your organization has an operational relationship. Third-party compromises may expose the organization's data, systems, or operations to risks and threats; this methodology aims to minimize the potential impact on your organization's information assets and reputation.

INCIDENT HANDLING STEPS

6 STEPS ARE DEFINED TO HANDLE SECURITY INCIDENTS

1. Preparation: prepare to handle the incident
2. Identification: detect the incident
3. Containment: limit the impact of the incident
4. Remediation: remove the threat
5. Recovery: recover to a normal state
6. Lessons learned: identify and improve the process

IRM provides detailed information for each step of the incident response process. The steps stem from the NIST Computer Security Incident Handling Guide.

PREPARATION

OBJECTIVE: ESTABLISH CONTACTS, DEFINE PROCEDURES, GATHER INFORMATION TO SAVE TIME DURING AN INCIDENT.

- Maintain an *up-to-date* inventory of all third parties, partners, providers and contractors with access to the organization's systems, data, equipment or infrastructure.
- Prepare and have a readily available contact book of people to involve when contracting third-party services.
- Define specific 24/7 contact points and people to intervene during non-working hours..
- Establish a process to assess the information system maturity of onboarded service providers via a KYS questionnaire.
- Establish and maintain Service Level Agreements (SLAs) with third parties, including security and incident response requirements; and specific alerting clauses in case of a compromise of a third-party.
- Regularly review and assess third-party security controls, policies, and procedures.
- Establish a formal map of interconnections and communication flows with service providers
- Implement a "Red Button" to cut off all IT links with the impacted service provider should such a need arise.
- Assess the feasibility, capacity and time required to block interconnection links with a third party, or third-party accesses; validate with tests and cut off exercises. Make sure to take into account business impact and regulator requirements.
- Regularly conduct joint incident response exercises with critical third parties.
- Prepare internal and external communication strategy in case of an incident including alternative communication channels for applicable contacts.
- Set up a watch process of ransomware shaming blogs and sites; conduct a comprehensive list of keywords, industry categories or geographies to apply to the desired watch process. Please note that depending on the country, research activities involving leaked data may be subject to compliance with local data regulations including GDPR and the penal code. Please check with your data protection officer, compliance officer or legal advisers prior to setting up the watch process. Conduct an active watch of known threat actors, particularly ransomware operators.
- Maintain regular monitoring of businesses that experience a cyber attack, especially those compromised by ransomware
- Automate internal alerting to notify on the presence of a partner on one of the sites of Shaming blogs.
- Prepare dedicated facilities for scanning or sandboxing of applicable data and files to use during the incident.

Additional legal requirements are to consider when setting up the monitoring process
e.g. https://www.cnil.fr/fr/la-recherche-sur-internet-de-fuites-dinformations-rifi

IDENTIFICATION

OBJECTIVE: DETECT THE INCIDENT, DETERMINE ITS SCOPE, AND INVOLVE THE APPROPRIATE PARTIES.

You may need to notify stakeholders, partners and regulators at the beginning of this step if required.

Detection

- Use proactive monitoring stemming from shaming blogs' watch, open sources or private notification: regularly check and analyze all applicable threat intelligence feeds for early detection of information on potential third-party compromises.
- Continuously monitor ingress / egress network flows to timely detect anomalies in interconnections with third-parties.
- Involve all previously identified stakeholders (Business, Purchasing, Legal, Infrastructure, Information Security, etc.); evaluate potential impact based on available information on the incident and feedback from the business and the IT.
- Evaluate possible remediation scenarios: blocking interconnections, reinforcing monitoring based on the risk assessment vs. potential impacts on production.
- Communicate/escalate the incident to higher levels in your organization (up to the Board) to have the most complete and comprehensive vision of the situation.
- Establish communication channels with the impacted third-party to share information about the ongoing incident. If required by the incident's nature, set up dedicated alternative (non-corporate) channels to use for communication and data exchange during the incident.
- Evaluate the level of provider's trustworthiness according to the level of transparency that can be established with the third party, perception of the quality of its communication and the effective delivery of applicable investigation and incident handling reports, IOC, etc.

Additional due care recommendations: in case of signs of lateralization, please refer to IRM 18 – Large Scale Compromise.

CONTAINMENT

OBJECTIVE: MITIGATE THE ATTACK’S EFFECTS ON THE TARGETED ENVIRONMENT.

If the incident involves access to organization’s sensitive resources, a specific crisis management cell may be summoned.

- Temporarily suspend or restrict the affected third party's access to the organization’s systems, data, equipment or infrastructure, as necessary.
- Limit communication by email completely or selectively (i.e. by redirecting provided emails to a dedicated sandboxed environment or mailbox, by stripping attachments, links, or other content).
- Set up regular meetings with the affected provider, onboarding applicable stakeholders.
- Coordinate with the affected third party to implement containment measures, such as isolating compromised systems, blocking malicious IOCs, or changing credentials.

If applicable to the obtained IOCs:

- Block traffic to C2s.
- Block any IP detected as used by attackers.
- Disable accounts compromised/created by attackers.
- Send the undetected samples to your endpoint security provider and/or private sandboxes.
- Send the uncategorized malicious URL, domain names and IP to your perimetric security provider.

If business-critical traffic cannot be disconnected, allow it after putting in place additional security controls to timely detect and inhibit lateral proliferation.

REMEDIATION

OBJECTIVE: TAKE ACTIONS TO LIMIT THE IMPACT ON PRODUCTION

- Reassess the transparency and applicability of the third party's remediation efforts.
- Consider requesting a formal incident report as applicable to the ongoing incident handling process or forensic investigation, i.e. a letter of commitment signed by the provider’s board or an investigation report by the incident handler / forensic service in charge of the incident.
- Request an up-to-date list of applicable IOC as reveled by the investigation process.

RECOVERY

OBJECTIVE: RESTORE TO NORMAL OPERATIONS.

All the following steps shall be made in a step-by-step manner and with technical monitoring.

- Obtain a formal report from a trusted third party ensuring that the claimant's situation is indeed back to normal.
- Decide with internally-identified actors whether reopening services, interconnections with the partner is feasible.
- Work with the affected third party to restore affected services or systems, ensuring that they are secure and free from vulnerabilities.
- Reevaluate and update the third party's risk profile in light of the incident.
- Gradually reinstate the third party's access to your organization’s systems, data, and infrastructure, ensuring that appropriate security measures are in place.

LESSONS LEARNED

OBJECTIVE: DOCUMENT THE INCIDENT'S DETAILS, DISCUSS LESSONS LEARNED, AND ADJUST PLANS AND DEFENSES.

Report

An incident report should be written and made available to all the stakeholders.

The following themes should be described:

- Initial cause of the infection
- Actions and timelines of every important event
- What went right
- What went wrong
- Incident cost
- Indicators of compromise

Capitalize

- Conduct a post-incident review with the affected third party to identify areas for improvement.
- Update applicable playbooks or incident management methodologies and other relevant processes based on lessons learned from the incident.
- Share lessons learned with stakeholders and security community actors to improve overall security posture and incident response capabilities.
- Keep relevant stakeholders within your organization informed throughout the incident response process, including senior management and the legal department.
- Make sure the incident has been properly documented, including timeline, impact, and response measures, for compliance and audit purposes.
- In coordination with the legal and public relations departments, prepare and release appropriate communications to external parties - if needed.