Incident Response Playbooks – Indispensable in Future Crisis situations

Tomaso Vasella
Defense Department, scip AG
tova@scip.ch
https://www.scip.ch

Marc Ruef (Editor)
Research Department, scip AG
maru@scip.ch
https://www.scip.ch

Abstract: Without a predefined playbook, a speedy and effective response to cybersecurity incidents is almost impossible. Playbooks are detailed, practical guides designed for specific situations. Playbooks focus on dealing with the consequences of an incident and not its causes.

Keywords: Complexity, Cybersecurity, DDoS, Detect, Exploit, Extortion, Forensic, Framework, Hacker, Logging

1. Preface

This paper was written in 2019 as part of a research project at scip AG, Switzerland. It was initially published online at *https://www.scip.ch/en/?labs.20190103* and is available in English and German. Providing our clients with innovative research for the information technology of the future is an essential part of our company culture.

2. Introduction

Cybersecurity events have unfortunately become part of *everyday life* and must simply be accepted as *common* occurrences. Even large, high-tech companies with lots of financial resources are not always up to the task of properly managing the number and complexity of attacks. This is why experts recognized long ago that for most organizations, it is simply *a matter of time* before they are faced with a successful cyberattack.

Once an incident has occurred, it is already too late to establish the necessary processes, resources and communication strategies for a successful *incident response*. Without appropriate plans in place, attacks might even go unnoticed, or the response might not employ the proper resources and channels, resulting in much greater damage than if thorough precautions had been taken from the outset. All of this demonstrates that a strong security strategy must include solid basic security and effective detection mechanisms as well as careful preparation for potential incidents.

3. What is an Incident Response Playbook?

When it comes to *incident response and recovery*, a distinction can be made between general aspects that apply to the organization as a whole and *specific* procedures to be implemented in certain situations. The incident response process itself is usually more overarching in scope, whereas incident response playbooks are *detailed procedures planned out in advance* to deal with certain incidents or problems. Typical situations addressed in playbooks, for example, include the handling of malware, phishing emails, and how to respond to DDoS attacks. In other words, incident response playbooks are *subject-specific practical guides* that describe the concrete steps to be taken in response to certain types of attacks or incidents.

Incident response playbooks are designed to swiftly facilitate *effective and appropriate action* during an incident in order to minimize the negative impact of cybersecurity incidents. In other words, they are a type of emergency plan and must be highly practical. As with any other critical incident, it is necessary to take measures ahead of time to identify the procedures, responsibilities, communication channels and resources that will be deployed. After all, when things heat up during a cybersecurity incident, you can't afford to discuss basic decisions or lose valuable time searching for phone numbers or passwords.

An incident response playbook is activated by a suspected or actual incident, contains the relevant procedures and defines the desired result. It should meet the following criteria:

- It pertains to a clearly defined incident (scope definition)
- It contains detailed, fully documented, standardized procedures
- It focuses on dealing with the consequences of an incident and not its causes
- The document and its language are easy to understand even under pressure
- The main focus is practicality
- It simplifies and helps to manage difficult decisions and conflicting goals, e.g. whether a system should be operational again as soon as possible or whether there first needs to be an investigation and collection of evidence
- It specifies rules for involving third parties, such as external experts, insurance companies, forensics specialists, government agencies, etc.
- It defines rules for external communications (PR, customers, business partners)
- It undergoes regular revisions and updates

4. Structure and Content of Playbooks

When responding to a cybersecurity incident, there is often an asymmetry between the attacker and the defender: the defender does not (yet) know the attacker's motives, the extent of the breach is unknown, the consequences cannot yet be assessed, etc. In other words, it is a very acute but reactive situation. You have to know what resources are available, who has the authority to make decisions, and what the consequences of these decisions may be. And, if possible, all of this should be documented and practiced before an incident occurs.

First and foremost, playbooks need to be *practical*. So there should be flexibility in terms of the structure and content, according to the particular application area. One tried and tested method is a structure based on the *Hacker Tools, Techniques, Exploits, and Incident Handling course offered by the SANS Institute* [1]:

1. Preparation
2. Identification, detection
3. Analysis
4. Containment
5. Eradication, remediation
6. Recovery
7. Lessons learned

These categories have proven effective in practice and, of course, can be simplified or combined into fewer phases depending on the situation.

4.1. 1. Preparation

The goal is to *prepare all resources and processes* needed to *manage cybersecurity incidents*. This means that many of the preparations are of a general nature and can be applied to all kinds of cybersecurity incidents. This might include process definitions, assembling the incident response team, central points of contact, detection and alarm channels, etc. It makes sense to manage this relevant but generally applicable information centrally.

This section of the playbook should therefore only include information relevant to the specific playbook application. A playbook for a DDoS attack, for example, would include detailed information about the mitigation procedures that had been prepared and would list the services that had been coordinated with the provider. In contrast, a malware playbook would contain information about the various mechanisms for protecting against, detecting, and analyzing malware incidents.

4.2. 2. Detection

When an incident is identified or there are any other critical indicators, *it is time to bring in the playbook*. This section of the playbook describes the detection mechanisms that have been implemented and appropriate reporting channels for the playbook scenarios. Usually, these are alarms in a monitoring or alert system such as an IDS or SIEM. Reports from users or third parties should also be considered, however.

The more specific and accurate the detection of an incident is, the more precise and efficient the response can be. In practice, a correlation between multiple indicators is often needed for reliable detection, and the line between detection and the subsequent analysis is often blurry.

4.3. 3. Analysis

The goal of the analysis is to identify *the actual and potential effects* of the incident. In other words, it is less about the cause and more about the consequences, because these are what determine the next steps in the playbook.

Perhaps the most important step in this phase is determining the criticality and business impact of the incident, as these aspects will affect the course of action. This usually occurs based on simple criteria presented in a table or decision flowchart correlating the criticality (usually three or four levels) with certain situations, systems, or processes. Typical questions here, for instance, are whether customer data has been affected, a breach of confidential data has occurred, or core business processes have been compromised. During this phase, there should also be a decision as to whether or not to collect evidence and whether this evidence needs to be admissible in court.

4.4. 4. Containment

The purpose of containment is to *prevent damage as quickly and effectively* as possible while also limiting its impact and further escalation. This part of a playbook consists of a list of technical and organizational measures to be taken. These are often in the form of an immediate solution; the permanent solution to the problem is usually implemented later after more detailed planning and in cooperation with other teams.

In the case of a malware playbook, this might entail scanning and isolating affected systems in the network. In the case of a phishing attack, it might involve sending out a blanket warning to potential recipients.

4.5. 5. Eradication, remediation

The solution should, on the one hand, *fully eliminate the cause of the damage* after it has been disabled in the previous phase. On the other hand, it should also eliminate the underlying problem that made the attack possible in the first place. This often involves turning the immediate solution into a more permanent, operationally viable solution. Remediation is usually a difficult task and can require one or a whole range of *measures* whose *effectiveness is measured over time*. The specific steps greatly depend on the focus of the playbook and the cause of the problem. They may range from installing patches to fully reconfiguring entire infrastructures.

4.6. 6. Recovery

Here the task is to *restore normal operations* for systems and infrastructure components. Logging, monitoring, and alerts should therefore be adjusted based on new information to ensure containment and remediation are actually successful while at the same time enabling the detection of any signs of new incidents early on.

After an incident, it can take time to restore normal operations. Using this time to plan ahead enables a swift,

focused recovery effort. It is extremely important to closely monitor and document activities during this phase to learn through experience just how much time is required for recovery. Ultimately, this knowledge helps to improve the effectiveness and efficiency of the recovery phase.

4.7. 7. Lessons learned

This final step is often neglected, perhaps due to the sense of relief after an incident has been resolved or because time is of the essence. But *there are lessons to be learned from every incident*, and it is very important to prioritize this phase appropriately, to reflect, and to document the experience. A good way to prepare for future incidents is by preparing an in-depth report detailing all of the observations and actions taken. Important questions that should be asked here:

- How and why did the incident occur?
- What might have prevented it?
- What technical and organizational security measures need to be changed or improved?
- Were mistakes made during the incident response, and how can these be avoided in future?
- Were any weaknesses identified in the process or organization?
- Was communication effective during the incident?

*What parts of the experience are worth sharing with a wider audience?

Ultimately, incorporating this knowledge into a continuous improvement process is very worthwhile. In doing so, both the playbook and the incident response process as a whole should be taken into account.

5. Which playbooks are needed?

Each organization is exposed to specific risks and has its own processes and organizational particularities. Playbooks are concrete, practical and, by definition, individual. In other words, the topics and content of the playbook have to be tailored to the specific organization. However, there are some main starting points for developing your own collection of playbooks:

- Malware outbreak
- Ransomware infection
- Dealing with phishing
- Dealing with data breaches
- Handling DoS attacks
- Dealing with cases of extortion
- Responding to unauthorized access
- Abuse of privileges, applications, and systems (insider incidents)

6. Conclusion

Every organization will be forced to deal with a cybersecurity incident sooner or later. In addition to solid basic security and appropriate mechanisms for detection, careful preparation for security incidents can make all the difference between an optimal damage control strategy and potentially fatal consequences. Incident response playbooks lay out specific, practical procedures for responding to cybersecurity incidents, making them an essential component of the incident response and recovery process.

6.1. Find out more

- *NIST Guide for Cybersecurity Event Recovery* [2]
- *NIST Computer Security Incident Handling Guide* [3]
- *Playbooks from the Incident Response Consortium* [4]
- *NIST Cybersecurity Framework* [5]

7. External Links

[1] https://www.sans.org/course/hacker-techniques-exploits-incident-handling
[2] https://www.nist.gov/publications/guide-cybersecurity-event-recovery
[3] https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
[4] https://www.incidentresponse.com/playbooks
[5] https://www.nist.gov/cyberframework