Incident Management Process for an Automated Teller Machine (ATM)

A Report by

Mark Kardash

SDEV360: Secure Software Engineering

Professor David Gabello

12 December 2023

University of Maryland Global Campus

Incident management is one of the most important aspects of the Software Development Life Cycle (SDLC). It is a detailed and thorough process of detecting, evaluating, and resolving issues in public and private software products. It includes guidelines, policies, tools, and other elements to help developers address issues like breaches and vulnerabilities (Makumbi, 2017). In this report, a hypothetical scenario involving an Automated Teller Machine (ATM) will be subjected to the process of incident management. Specifically, the paper will look at the actions of a team after the same User ID retrieved large amounts of money from a group of networked ATM systems. Some processes for reporting and acting upon the issue will be listed, as well as processes to ensure that the issue has been resolved effectively.

According to Atlassian, the first steps in the incident management process are identifying and logging the incident (n.d.). The ATM issue would most likely be identified very quickly, as the bank tracks all transactions made on the machine. It would have been spotted by one of the people involved with authorizing the transactions. For the sake of this report, this will be an ATM operator. Logging essentially means documenting the problem at hand. Some of the things included in an incident log are: The name of the whoever is reporting the incident, date and time of the report, an incident description, and a tracking number (Atlassian, n.d.). It may also include the name of the supervisor. An incident report log of the ATM breach may look something like this:

Golden Fleece Bank

Incident Report

|  |  |
| --- | --- |
| Reported By: | Mark Kardash |
| Position: | Automated Teller Machine Operator |
| Supervisor: | David Gabello |
| Date and Time of Incident (MM/DD/YYYY,  HH:MM). | 12/09/2023, 16:08 |
| Incident Description: | A single User ID was used to withdraw a total of USD 2,780,000 from 5 of the ATMs in the Golden Fleece Bank Network. |
| Tracking Number: | 4027105533821 |

After the report has been filed, it must be categorized according to its nature. Each company may have different categories in its policy (Atlassian, n.d.). Categorization helps the development team organize issues, making it easier to handle them. This is because it helps them find patterns and trends, thus identifying common elements, and reach a resolution faster (Atlassian, n.d.). Since it appears that a single user managed to infiltrate the entire network and take advantage of several machines, the ATM incident can be placed into a “Breaches” category.

While categorization may be very easy if certain characteristics of the issue are effectively identified, the next step of the process, Prioritization, requires a much more in-depth analysis. In simple terms, to prioritize an incident is to base the team’s approach to it on its severity. But there are many intricacies that go into this seemingly easy task. Severity is not only determined by “how bad” an issue is, or how it could damage the network. The evaluation usually has several stages: Measuring the incident’s impact on the company, determining the number of people it will affect, calculating potential financial losses, considering security risks it poses, and understanding its implications for compliance. It also involves comparing it to other incidents, which will not be done here due to the absence of such incidents. This paper will apply the ATM incident separately to each one of them.

To determine how the ATM breach will affect the hypothetical Golden Fleece bank, the issue must be once again stated and examined. To recap, developers are faced with the following incident: Significant amounts of money were retrieved from multiple ATM’s belonging to the bank’s network, by a single individual, as indicated by the User ID. First and foremost, just like any breach, this points to serious shortcomings in the security of the system, which is never good news for a company. When placing their funds into a bank, customers want, and expect, for them to be safe. Should the incident go public, customer trust will be severely shaken. In the long term, this means significant customer loss, and therefore, financial damage. In addition, should the attacker have gained access to personal customer information, the situation would escalate into a case of identity theft, bearing catastrophic consequences. Hackers may use the information they stole to access even more financial resources using the names of their victims. Thus, a single ATM incident can very easily give rise to a wave of crime.

Aside from the fact that its reputation will be tarnished, the bank may now need to spend large sums of money on security improvements, such as better firewalls and password encryption methods. This may put the bank into an even more difficult position financially. With what is known from the description of the incident, it is impossible to calculate the exact number of people it will affect. It can only be assumed that all the customers at the bank will be impacted, due to the trust issues that will arise. However, the ones impacted the most would be the owners of the accounts from whom the cash was taken. Losing their funds may even lead some of them to sue the bank, putting it into an even more dire situation financially. The situation will also affect the ATM operators who were responsible for authorizing the transactions, leading to potential firings, quitting, and shortages of staff. All of this will put immense pressure on the bank’s CEO, who, as the one in charge, would have to practically carry the situation on his shoulders. There are no details on exactly how much money was retrieved from the machines (The number given in the report is just a stand-in), how the attacker penetrated the security measures, how much customer information they may have in their hands, or how quickly the issue can be resolved. All these factors determine how much the incident will be publicized in the news. The CEO and other bank officials may need to give many interviews and give explanations for multiple aspects of the story. The more publicity this incident receives, the more it may end up hurting the bank.

The security implications of this incident have been largely described above, but any kind of breach or attack would mean that the bank’s ATM system is no longer safe. Extensive checks would need to be run on the software, to ensure that no additional, unnoticed issues exist. If they do, a plan of action would have to be developed to address them. As mentioned above, appropriate tools would then need to be chosen for handling them.

Regarding the incident’s implications for compliance, the bank may need to perform a major review and overhaul of its security policies. They will need to ensure that their security measures meet the standards outlined for their organization, and, if necessary, make updates for their software to meet those standards.

Now that each piece of the puzzle has been analyzed, the incident could finally be properly categorized. For this purpose, incident severity will be divided into Low Risk, Medium Risk, High Risk, and Critical. Because of its severe impact on data integrity, fund security, along with the bank’s reputation and financial well-being, the ATM breach would most definitely fall under the Critical category. Such incidents require special attention and are addressed before all others.

After Categorization comes the most extensive, most intricate part of the Incident Management process: Response. To effectively respond to any issue, teams must first correctly perform all the steps above, as they are just as crucial for this. Just like Categorization, Incident Response is composed of several stages: Initial Diagnosis, Escalation, Communication, Investigation and Diagnosis, Resolution and Recovery, and Closure (Atlassian, n.d.). To make the distinction easier, this report will dedicate a separate section to each process.

**Initial Diagnosis:**

This stage is essentially the same as the very beginning of incident management. If team members are unsuccessful with detecting and diagnosing an incident, they will log and escalate it to the next team (Atlassian, n.d.). While the nature of the ATM incident is quite clear, the team responsible may want to escalate it to a higher management for more effective handling.

**Escalation:**

In this stage, the incident log is escalated to the Incident Manager, who gathers a team to resolve the issue. Since it is a breach, after detecting the exact vulnerability in the system, they would need to use a patch to fix it. Escalation can be a continuing process, as the incident can be handed over to teams multiple times until one of them manages to resolve it (Atlassian, n.d.). Each team must act as quickly as possible, due to the categorization of the incident as Critical. For this scenario, each team will get a maximum of two hours for resolution.

**Communication:**

As the team looks for ways to resolve the ATM issue, they will frequently share progress updates with those impacted by the crisis. They will mostly be the external and internal stakeholders of the bank (Atlassian, n.d.). Keeping these individuals in the know is essential to maintaining their trust despite the stress of the situation. For instance, they may contact them to let them know about the possible theories of what may be causing the issue, or notify them when the issue is finally resolved. While not much is known about the breach in question, the teams would most likely let their stakeholders know if they found out exactly what personal information was stolen, and what dangers may come from this. The most effective way to communicate the issue and resolution to the stakeholders would be to send them a company message, such as a professional email.

**Investigation and Diagnosis:**

This is a deeper dive into the issue than what is done during initial diagnosis. For the final diagnosis, developers often turn to additional resources, such as experts or tools, if they are unable to identify the threat initially (Atlassian, n.d.). To detect the ATM breach, the teams may contact their superiors, such as the Team Lead or Manager. In addition, they may use several digital tools, such as:

* ManageEngine Export DLP Plus: A tool that scans the system to detect breaches and vulnerabilities, places them into categories, and implements solutions (CompariTech, 2023). Such a tool would make the process much shorter, as it would also automate the Categorization stage.
* ESET-Project: An antivirus-like protection software that is essentially a private network for threat intelligence. It provides multi-level protection of the system, detecting breaches, coordinating, and handling pooled threats. It works on multiple systems, such as Windows and Mac OS, as well as on mobile devices (Cooper, 2019).
* UpGuard BreachSight: This useful tool not only detects breaches, but also protects system data and credentials (Cooper, 2019), which is especially useful in this scenario. It is Cloud-based and protects against threats like credential disclosure and data leaks, by using a scanner that alerts the team to any problems found. It detects running processes to act immediately if a cyberattack is in progress (Cooper, 2019).

**Resolution and Recovery:**

After the long series of preparatory steps, comes the Resolution and Recovery phase. Resolution is, quite simply, the process of fixing the issue, while recovery refers to the amount of time the system will need to be fully operational again (CompariTech, 2023). As mentioned in the “Escalation” section, to resolve the issue, a patch would be applied in the affected area, after the damage has been assessed. The team would then notify bank officials and stakeholders to watch out for any service disruptions or suspicious activity. An email sent to them would also contain clear instructions for how to behave to ensure that the issue has indeed been fixed, such as a number to call to report unauthorized transactions, changing their PIN, and letting a certain number of hours pass before their next use of the machine.

**Closure:**

This is the easiest part of the entire process, as now that the incident has been resolved, the team in charge passes it to the service desk, where it is declared closed (Atlassian, n.d.). This happens only after the person who initially reported the incident confirms that they are satisfied with the solution and can be done only by the employees at the front desk, to avoid any confusion, disruptions, or complications in the Incident Management process (Atlassian, n.d.).

**Potential Additional and Follow-Up Processes:**

Before resolution can begin, developers must gather as much information about the incident as possible. This additional measure is needed for future reference, as it will help developers in dealing with a potential recurrence of the issue, or occurrence of a similar one, in the future. In the case of the ATM breach, the recordings should contain very important details, such as what information was stolen, how much money was stolen, the time of resolution, the cost of resolution, as well as what measures were taken against the issue. To minimize the recording efforts during this phase, developers should record as much information as possible during the initial logging process. To simplify the current resolution phase, developers should look through previously recorded issues to see if the breach has occurred before. If it has not, then teams may end up spending much more time detecting the issue.

After the documentation is done, developers should review the incident and process for the final time, to ensure that it has indeed been adequately resolved and documented. They may also monitor the system for previous incidents, to ensure its safety in the future.

**General Conclusion:**

Incident Management is an imperative process for the Software Development Life Cycle. Without it, a plethora of companies would be experiencing major PR disasters, sinking in public outrage and lawsuits from unresolved issues in their systems. Clear policies, along with competent staff and efficient tools, can make Incident Management easier and more effective, saving a company’s time, costs, and reputation.

References

Cooper, S. (2019, November 1). *11 best breach detection systems for 2023 (Paid & free)*. Comparitech. Retrieved December 12, 2023, from <https://www.comparitech.com/net-admin/best-breach-detection-systems/>

*Incident management best practices and tutorials*. (n.d.). Atlassian. <https://www.atlassian.com/incident-management#it-style-incident-management-process>

Makumbi, A. (2017, March 8). *Incident Management and Patch Management*. GitHub. Retrieved December 9, 2023, from <https://makumbi.github.io/output/blog/2017/incident-management-patch-management.html#:~:text=Incident%20management%20and%20patch%20management%20plans%20developed%20early,mitigated%20or%20is%20restored%20as%20quickly%20as%20possible>