BRIEFING NOTES

#BN-40-Cyber and space as key enablers -Feb2021

INCIDENT RESPONSE PLAN

Authors: Reza Bahrevar[1] and Kash Khorasani [2]
[1] Graduate student, Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada
[2] Professor, Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada

SUMMARY

- Incident response plan is among the most essential tools in the cybersecurity strategy.
- An incident response plan is a documented, written plan that outlines what steps should be taken, and by whom, within an organization to deal with a data breach or cyberattack.
- It is important to specify and detail the roles of everyone on the incident response team, and clearly define each team member's responsibilities. In the event of an incident, having this clarity will minimize the confusion when difficult decisions will need to be made.
- Emergency responders would perform regular simulations for training, updating the process checks so that they can almost instantaneously act when a situation develops.
- An incident response plan should be set up to address a cyberattack in a series of phases that are comprised as follows: 1- Preparation, 2- Identification, 3- Containment, 4- Eradication, 5- Recovery, and 6- Lessons Learned.

CONTEXT

- Solidifying a cybersecurity strategy is becoming more important than ever since one is witnessing many attacks over the past few years. In view of this fact and the prevailing trends in cyberattacks, prevention, detection and response policies are three essential challenges that we need to be considered with in articulating our cyber security strategy.
- As discussed in previous BN reports (i) prevention, (ii) detection and (iii) response are three essential attributes that one needs to consider in cyber security strategies. The last step is response. After one has set up the wall of defense, and it is penetrated, one has to be the one fully prepared for a response, reporting, and remediation. That is why we consider security arrangement and incident response processes as the most essential tools in one's cybersecurity strategy and security operation.
- An incident response plan is a documented, written plan that outlines what steps should be taken, and by whom, within an organization for dealing with a data breach or cyberattack.
- This is a plan to ensure an organization is ready to detect, respond to and recover from a cyber incident. A robust response plan should mitigate damage to the system as quickly as possible.
- Emergency responders perform regular simulations for training, updating and processing checks so they can act almost instantaneously when a situation develops.
- Information security teams are highly advised to follow their example: when an emergency occurs, one will not waste time identifying processes and procedures for incident response, while valuable minutes ticking away. It is imperative and essential to have a plan in place.

CONSIDERATIONS

Incident Response Plan

- The last step in the cyber strategy is response. After one has set up the wall of defense, and it gets penetrated, one has to be equipped with tools for a response, reporting, and remediation. That is why one should consider security arrangement and incident response process the most essential tool in the cybersecurity strategy and security operation.
- An incident response plan is a documented, written plan that outlines what steps and by whom should within an organization actions be taken to deal with data breach or cyberattack. This is a plan to make sure the organization is ready to detect, respond to and recover from a cyber incident. A robust response plan should mitigate damage to the system as quickly as possible. Emergency responders perform regular simulations for training, updating and process checking so they can act instantly when a situation develops. Information security teams would be wise to follow their example: when an emergency occurs, one should not waste time identifying processes and procedure for incident response, while valuable time passes. It is essential to have a plan in place.
- To create are acceptable incident response plan, one needs to consider various phases when a cyberattack or a data breach have occurred in the organization.
- **Preparation:** This is the most critical phase in the incident response plan to protect one's organization. The response plan should be well documented, thoroughly explaining everyone's roles and responsibilities. It is essential to test the plan and make sure that all stakeholders understand their roles and can act as trained.
- **Identification:** When the organization has been attacked it is important to realize the originate of it, how it was discovered, the compromise scope, the affect and impact of the attack on the systems and severity of it. Discovery of the source (point of entry) of the event can also help one to prevent it in future.
- **Containment:** If a breach is detected first, the initial instinct may be to delete everything securely so that one can get rid of it. This would, however, potentially is not advantageous in the long run since one would lose valuable evidence that needs to determine where the breach has initiated and establish a strategy to avoid it.
- One should contain the breach instead, so that it does not propagate and cause further damage to the organization. Have containment strategies ready for short-term and long-term. A redundant system backup is also desirable for helping one to restore normal operations. Thus, no data is ever lost if it is compromised. It is also a perfect time to upgrade and patch programs, check the Remote Access Protocols, add multi-factor authentication to the checking process, change the user's and administrator access keys and harden one's passwords.
- **Eradication:** The nest phase after containing the issue is to find and eliminate the breach's root cause. All malware should be removed, systems should patch again with the updates.

If any trace of malware or security issues remain in the systems, one may still be losing valuable data. Therefore, going through the entire system is needed. To do so maybe the organization needs to hire a third party to conduct these activities.

- **Recovery:** In this phase all the affected systems and devices return back to normal operation. It is very important during this phase to monitor all the affected systems by tools such as File integrity monitoring, intrusion detection/protection for a while to get one's systems and operations up and running again without the fear of another breach.
- **Lessons Learned:** Upon completion of investigations, have an after-action meeting and discuss the findings with all the members of the Incident Response Team. This is where everything about the attack is analyzed and documented. Determine how good the action strategy has performed and where there were some inadequacies. Learning from mockery as well as real events will help strengthen one's systems against future attacks.

Cyber Security Awareness Program

- As far as cyber security strategies, the most crucial and the first step is prevention. The most important element in prevention is awareness of risks and threats and their domain. Individuals play a critical role in helping to reduce organizational risks associated with cyber-attacks. Whether it is through careless handling of sensitive data, falling for phishing attacks, or poor password management, many data breaches are directly or indirectly caused by user awareness issues.
- It is therefore essential that organizations have a formal security awareness program in place to ensure employees are aware of the importance of protecting sensitive information, what they should do to handle information securely, and the risks of mishandling information.
- Best Practices in Organizational Security Awareness Program can be listed as follows:
- **Assemble the Security Awareness Team:**
  This team is responsible for the development, delivery, and maintenance of the security awareness program. The team should be staffed by employees from various areas of the organization, with different responsibilities representing a cross-section of the organization.
- **Determine Roles for Security Awareness**
  Role-based security awareness offers organizations a guide to train workers at acceptable stages, on the basis of their work duties. The goal is to create a reference list of various expertise and training depths in order to assist organizations with training the right people at the right time. The first challenge in designing a role-based security awareness program is to define responsibility levels and group members according to their positions (jobs functions).

- **Security Awareness throughout the Organization**

  An approach to a successful security awareness program is to provide relevant content in a timely and secure manner to the appropriate audience. The communication channel should also fit the culture of the organization in order for it to be effective. The organization ensures that employees are subjected to the same information several times in various ways by disseminating safety awareness training via several communication channels. This greatly improves how people will remember the information that are presented to them.

REFERENCES

1- https://www.cisco.com/c/en/us/products/security/incident-response-plan.html
2- https://www.cmu.edu/iso/governance/procedures/docs/incidentresponseplan1.0.pdf
3- Lucie Hayward and Michael Quinn, “It’s Not If But When: How to Build Your Cyber Incident Response Plan”, Cyber Security of Kroll companies
4- https://www.rapid7.com/fundamentals/incident-response-plan/
5- Brady, "Emergency management: capability analysis of critical incident response," Proceedings of the 2003 Winter Simulation Conference, 2003., New Orleans, LA, USA, 2003, pp. 1863-1867 vol.2, doi: 10.1109/WSC.2003.1261645.
6- Charles DeVoe, Shawon Rahman “Incident Response Plan for a Small to Medium Sized Hospital” Cryptography and Security, 2013
7- DAVID ELLIS, https://blog.infogressive.com/6-phases-of-incident-response#:~:text=Incident%20response%20is%20typically%20broken,eradication%2C%20recovery%20and%20lessons%20learned.