CS 542 – Introduction to Software Security
DHS Tabletop Exercise

Binhao Chen (bchen276@wisc.edu)

November 3, 2022

1. What are the major steps that take place in the incidence response to a cyber attack? Anything special or different for a ransomware attack?

In my opinion, the incidence response to a cyber attack is a series of systematic network/information security policies, methods and procedures. These systematic steps can be used to identify, contain and neutralize cyber attacks. After doing some research and research, I found several standard operating procedures for dealing with cyberattacks, among which the National Institute of Standards and Technology (NIST) and the Escal Institute for Advanced Technology (SANS Institute) developed two of the most respected incident response frameworks that provide the foundation for IT teams/organizations to build an incident response plan[cro22]. They divided the steps that take place in a cyber attack incident response into 4 main parts:

1. Preparation of systems and procedures
It is difficult for most victims to initiate an effective incident response immediately upon notification. They must develop a specific set of plans to prevent and respond to incidents. The most effective and precaution action is to form and maintain a computer security incident response team that includes technical experts empowered to take action in support of the business, as well as representatives from management, technology, legal, and communications disciplines. In this way, in emergencies, everyone can perform their own duties and cooperate to minimize the adverse impact.

2. Detection and and Analysis of incidents and threat
The main task in the second step is to detect and analyze the severity and type of cyber attacks suffered. Once identified, the corresponding Rapid Response Unit must begin documenting all facts related to the incident and continue documenting all actions and analysis taken throughout the process. They must score incidents based on their impact on business functionality, the confidentiality of affected information, and the recoverability of the incident. They also should notify the appropriate departments/ units to better prioritize the attack and reduce the overall damage suffered from the attack

3. Investigation into the origin of attack, Eradication of attackers and re-entry options, and Recovery from incidents, including restoration of systems
The main goal of the third phase is to reduce or even completely stop the impact of the incident before it causes further damage. When the scope and impact of an attack is under control, the team responsible for cybersecurity can then proceed to take the necessary steps to address the root cause of a similar attack and restore operations and operations to normal. These processes should be documented so that the team can learn from the attack and increase the expertise of the security team.

4. Post-incident: Lessons learned to the next round of preparation
The follow-up of each incident should be an opportunity to learn and improve. The team responsible for cybersecurity needs to be constantly updated to learn the latest technologies and coping strategies, and if necessary, involve people from the entire organization in the learning. Lessons learned can also be used to update policies and procedures and create institutional knowledge that can be useful in future events.

A ransomware attack is a malicious software (malware) that threatens to release or block access to data or computer systems until the victim pays the attacker a ransom. The main difference between the response to a ransomware attack and a general cyber attack is that an official or government investigative agency, such as the FBI, is usually invited to investigate and help the mitigation procedures in the early stages of the attack.

2. What is typical job of your role? Answer this question here by talking about the normal tasks and responsibilities of this job.

My role is Wisconsin National Guard. The Guard has a dual mission with both federal and state responsibilities. The typical job of the National Guard is to support active duty military forces in responding to threats abroad and humanitarian disasters. But, unlike most of the other military forces, it can also serve a domestic law enforcement role. In peacetime, the Guard is commanded by the governor. Domestically, they protect domestic communities at the state level [22a], which can range from armed insurrection to natural disasters. Each state has its own National Guard that the governor can call in in an emergency. The Guard also responds if the president asks them to serve the federal government. In local or statewide emergencies such as storms, water flood, and COVID-19, they are also pivotal in supporting the mitigation actions [22b]. Their work/job may also related to intelligence, technology, engineering, aviation and many other fields.

3. What is job of your role during a cyber incident response? What are your responsibilities? What decisions will you have to make? Who will you need to talk with and depend upon during an incident?

There is a team in the National Guard dedicated to preventing and dealing with cyberattacks. They can not only perform defensive operations, but also achieve the purpose of maintaining network security through offense. Their specific work/job and responsibilities includes [KR21]: 1. Execute cyber attack/defense, 2. Execute on designated systems and networks cyber intelligence, surveillance and reconnaissance operations 3. Conduct cyber terrain audits, penetration testing, basic digital forensic data analysis, and software threat analysis 4. Respond to cyberspace incidents, leverage cyberspace defense infrastructure capabilities, collect basic digital forensic data, provide incident response impact assessments and generate cybersecurity posture assessments

In the event of natural disasters such as hurricanes or tornadoes, the National Guard often works with critical infrastructure such as power grids or water supplies, and is equally able to support these infrastructures in advance of or in response to a cyber event. National Guard support for cybersecurity facilities includes cyber incident response and remediation; cyber defense analysis; cyber incident response planning; election security planning, threat assessment, and interagency planning [22b]. They need to decide on the prioritization of multiple simultaneous attack, specific mitigation actions, as well as the interagency work among many government/private sectors. When responding to cybersecurity threats, the Guard typically needs to conduct more assessments and other interactions with key critical infrastructure vendors, and increased communication and engagement with technologists from cybersecurity, cloud computing and telecommunications companies.

References

[22a] *Army National Guard*. Nov. 2022. URL: https://en.wikipedia.org/wiki/Army_National_Guard.

[22b] *National Guard*. Nov. 2022. URL: https://www.nationalguard.mil/About-the-Guard/Army-National-Guard/FAQ/.

[cro22] crowdstrike. *INCIDENT RESPONSE PLAN: FRAMEWORKS AND STEPS*. 2022. URL: https://www.crowdstrike.com/cybersecurity-101/incident-response/incident-response-steps/.

[KR21] Franklin D. Kramer and opinion contributors Robert J. Butler. *Expanding the role of the National Guard for Effective Cybersecurity*. Apr. 2021. URL: https://thehill.com/opinion/cybersecurity/550740-expanding-the-role-of-the-national-guard-for-effective-cybersecurity/.