A Cyber Incident Response Plan

Before we implement the DIAMOND system, it is crucial to draw up an incident response plan. The plan is supposed to include strategies to possible foresee risks and attacks to the system. This essay is to propose a reasonable plan for dealing with prevailing kinds of Cyber Incidents on the DIAMOND system.

According to oodrive[1], there are 10 well-known types of cyber incidents: Denial of Service (DoS) attack and Distributed Denial of Service (DDoS) attack, Malware, Phishing, Dive by Download, Password cracking, Structures Query Language, Man in the Middle (MitM), Cross-site scripting, Eavesdropping and Birthday attack. The common goal of these malicious activities is either to steal the information or to cause damage to the property. In this Cyber incident reponse plan, we discuss the solutions from four aspects: preparations, technical protocols, strategic decisions and stakeholder communications.

1. Preparations

Preparations are the behaviours before an cyber incident happens.

1. Make sure all the staff is trained so everyone understand the security protocols.
2. Regularly organizing system security audit, consulting professional security office to test attacks on the system.
3. Make sure every protocol that has been made is valid and up-to-date (in case of system architecture changes).

2. Technical Protocols

The DIAMOND system runs technical protocols immediately after perceiving abnormal online transactions (any activity that violates ACIDity of the system). These protocols are basically a set of programs that deal with different situations. The technical protocols consist of: incident sniffer, system suspension, backups and recovering policy.

Incident sniffer

The incident sniffer is responsible for detecting unusual activities happen to the system. The sniffer is built inside the proxy server. Since every data request goes through the proxy server, the sniffer can work with the server firewall to make a prelimary evaluation of data requestor (e.g. Whether the request is from an foreign IP address and this IP address has never appeared in the system before. Or whether the velociy of requesting is greater than the nomal operation velocity so it could probably be a machine crawling data). Any abnormality triggers alerts to the system manager, and the alerts show on the dashboard.

System Suspension

When the system manager confirmed that the sytem is under an known/unknown cyber incident, system suspension protocol can be launched. This protocol suspends the operation of the system. All servers will go offline except the server that only receives and saves data (e.g. The offline local server that saves data from speed and photo cameras).

Backups

Backup protocol runs 24/7. It is the protocol of the git repository mechanism of the system. Every server is equipped with an individual git repository, and it backs up the data on the server automatically on a regular basis.

Recovering Policy

The recovering policy will start the backup and recovery mechanism, and return the system to a certain point in time through periodic backups to ensure that the impact of cyber attacks on the system is minimized.

3. Strategic Decisions

When cyber incidents happened, apart from the technical aspects, there are decisions that are supposed to be made within the management cohort. These are instructions that the people work with the DIAMOND system should follow when cyber incidents occurred.

1. Keep records of the cyber incident, including species, time point, estimated losses, etc.
2. Do an analysis after every cyber incident, find out the reason why the attack was not detected or successfully banned, how can the system be updated.

3. Encapsulate the system breach, e.g. cut down the internet connections of the server that has been penetrated.
4. If the impact of the cyber incident is fatal, it might lead to an engagement with the media. Prepare for possible interviews.
5. Figure out exactly the the cause, process, results and solutions to the incident, and make them into an integrate report for stakeholders.

4. Stakeholder Communications

References

[1] Oodrive. (2021). *Top 10 of the different types of cyber attacks*. [online] Available at: https://www.oodrive.com/blog/security/top-10-different-types-cyber-attacks/ [Accessed 17 Dec. 2021].

Reflecting on the guest lectures

Topic/Guest	Reflections	Compulsory for the respective module y/n
Meat the Machine - Professor Colin Williams	In fact, sometimes the boundaries between humans and machines are blurred. Although humans create machines, machines cannot become humans. But human behavior patterns sometimes resemble robots. We can possibly understand what could be a good way to deisgn a piece of software by accepting this concept.	y
General and IoT attacks - Tony Gee	IoT attacks are sometimes not in the way that people would expect, it is much easier to cause information leakage. Everything that carries personal information possesses the probability of being hacked.	y
Supply chain security - Sarah Clarke	It is important that we keep essential informations in written documents. So when we need to aid, prioritize or plan, we would have the data to analyse.	y
Leadership - Alan Jenkins	Real leadership for the leader is about telling your people what to do. It is about making decisions for the group. However, sometimes I tend to do all the jobs when I'm a leader in the real life.	y
Resilience - Tim Armit	To ensure the business continuity and resilience, and to encounter with disasters, it is a thing about reflecting on plans frequently. Try to ask more questions about the system, so we're able to make adjustments in time.	y
Legal and regulatory aspects - Shavana Haythornthwaite	It is vital to do things in accordance with regulations and laws. The legislations are not only constraints for us, it is rather a powerful weapon to protect what we have.	y