The Critical Need for Information Security

Author

Institution

The Critical Need for Information Security

Cyber-attack is a kind of attack that tends to destroy, alter, steal, expose, disable or gain unauthorized access to computers or computer networks. Besides, one purpose for launching a cyber-attack could be; to hack into a susceptible system or use any organization’s asset with unauthorized access. Computer geeks are of the view; in order to protect any organization, computer, or a computer network from a cyber-attacker/hacker a network designer should act and think like the hacker. Cybersecurity management is no less than a military exercise. So, for that purpose new proactive processes and techniques, for countering cyber-attacks, have been introduced within this corporate battlefield. One of the proactive techniques that organizations use to counter cyber-attacks is a cyber-attack simulator system.

# Cyber-Attack Simulator System and its Advantages

One of the many news people come across in contemporary digital era is a cyber-attack. It disturbs the business, damage the reputation and panic end users. The days are long gone when cybersecurity management had to rely on an annual or quarterly penetration test results. In the current era, there is a need for an automated breach attack simulation (BAS), continuous assets scanning and of course protection. Cyber-attack simulator system is a sequence of steps leading to vulnerability identification on an information system (Kuhl, Kistner, Costantini, & Sudit, 2007). Cyber-attack simulator system reviews known vulnerability, and any known vulnerabilities are a potential path to cyber-attack.

As far as the advantages of cyber-attack simulator system are concerned; following are some advantages that would help organizations to secure their networking perimeter effectively and efficiently.

1. Cyber-attack simulator system identifies all the security gaps in the computer network or IT infrastructure of any organization. Besides, it is more or less similar to the penetration testing or, more precisely, the red team operation.
2. The basic purpose of red team operation or penetrating testing is to identify all the vulnerabilities in a specified time. However, with a cyber-attack simulator system, critical exposures in a network or IT infrastructure will be identified continuously by coupling red team operation with automated simulation testing (Kuhl et al., 2007). Cyber-attack simulator system ensures that there is no occurrence of time-lapses during the testing.
3. Following the identification of security gaps and vulnerabilities attached to a network, cyber-attack simulator provides cyber-security management with actionable and prioritize remediation (Kuhl et al., 2007). The remediation process identifies and addresses the weaknesses in the IT infrastructure.

# Sectors that have Greater Insight on the Potential of Cyber-Attacks

Insight on the potential of cyber-attacks greatly depends on the sectors such as criminals, government-funded (whether black or transparent), and/or commercial. In terms of criminals, there is a lot of illicit activity going around in the U.S., Eastern Europe (Ukraine, Russia), the Middle East (Saudi Arabia, UAE, Israel, and Iran) and Eastern Asia (China, Both Koreas, and Japan). And 90% of the attacks that happen every day, most them are phishing scams and simple malware distributions (Sandoval, Sapankevych, Santos, & Hassell, 2013). Each of the countries mentioned is equal in terms of the level of sophistication involved in attacks.

For the government, there are few parts involved but in terms of surveillance/data gathering, the United States has a huge advantage in terms of getting intel. Not only the U.S. has tremendous amount of money and an existing logistics program to deploy massive amounts of software and hardware (whether it's legal or not) for blanket surveillance and data collection, there are also collaborations with commercial companies. It's because if you look into the documents from the Snowden Revelations, the U.S. government (Along with the Five Eyes alliance) has a lot of connections with companies that handle massive amount of global data (Facebook, Google, Microsoft, etc.). The U.S. also has some of the best commercial technologies available (unrestricted in terms of usage because the tech isn't imported/exported) (Sandoval et al., 2013). So, combined with the tremendous amount of money, the tech, logistics (Such as the US Postal Service cooperating with the NSA in their TAO), and commercial connections, the U.S. cannot be beaten.

Another aspect of the government contributing to cybersecurity which is being involved in the consumer/commercial/enterprise world, I would still say the U.S. beat everyone else. The N.S.A. can take credit of creating the Security-Enhanced Linux kernel, which is extremely beneficial to anyone that utilizes it. The U.S. Air Force also released Portable Lightweight Security; a lightweight Linux distribution focused in portable security to the public. The U.S. Government also releases open-source encryption methods and algorithms that anyone can dissect, change, and/or utilize directly. I don't know any other country that has influence and contribution in the consumer/commercial/enterprise world than the U.S. I didn't even touch DARPA, The U.S. Armed Forces, or other government branches. For commercial technology, a lot of them are located and based off of the U.S. Other companies involved in security also get purchased by U.S. corporations /conglomerates. There are very good non-U.S. security companies like Kaspersky Labs (Russia), AVG Labs (Czech Republic), Trend Micro (Japan), and some others but again, most of them are in the U.S.

# Cyber Security Strategy

The most important elements of any cyber-security strategy are as follows:

1. Identify an executive sponsor. Without buy-in at the board level, the breach response plan will not be effective.
2. Identify key personnel that are part of the “Breach Response Team”.
3. Define clear responsibilities for each team member
4. Set communication protocols. Who will communicate project status internally? Who is responsible for communicating externally with the media and regulatory authorities?
5. Document and understand reporting requirements for data breaches in one’s own jurisdiction.
6. Identification of the type of cyber-attack.
7. Contain the cyber-attack so it does not spread or get worse.

There is no need to assign all of the incident response team members to the attack. In lieu, holding back a few team members to monitor the entire environment looking for other attacks is one of the best strategies, one should resort while countering the cyber-attack. Cyber-attacks can come in waves, for example, the initial wave would cause the incident response team to divert all resources to focus on the attack - most of the time the initial attack will be “loud” such as a massive DDoS attack designed to be big enough that the entire business and customers are demanding a quick fix, forcing the entire IT team to drop everything and focus on the attack (Rowe & Gallaher, 2006). While the DDoS is being run the baddies will commence another attack that is stealthier and more focused solely on getting into the environment. Assuming no one is watching, the baddies can try several attack vectors that may show up on the monitoring tools but be instantly drowned out by the DDoS alerts or considered by the business to be an issue caused by the DDoS attack.

# Cyber Security Plan

A good cybersecurity strategy primarily understands all of the requirements based on which the strategy would be created. Some of the requirements are delineated as:

1. Business strategy
2. Legal, regulatory and contractual obligations
3. Organization’s security risk exposure
4. Suppliers and partners
5. Customer needs and expectations
6. Internal and external contexts
7. Industry-specific standards
8. Security culture of the organization.

Once an action plan is determined to address these requirements, a sound security strategy can be created. The strategy could fail, due to these reasons:

1. Lack of a comprehensive understanding of the internal and external context of the organization.
2. Misjudging the security culture of the organization.
3. Poor implementation.
4. Not engaging the stakeholders early in the game.
5. Lack of management involvement and commitment to security projects.

A good indication of a good cybersecurity strategy is that the strategy requires minimum rework. Any investment made is always reused in the strategy revisions, and not thrown away (Rees, Deane, Rakes, & Baker, 2011).

# Importance of Public-Private Partnership in Cybersecurity

Public-private partnership is just like the involvement of private guns in public armor shop and then parallelly shooting out the competitor. Cybersecurity threats and risks are inevitable to deal with, in order to strengthen the security of a nation. There is fundamental uncertainty attached to cyber-security risks that not only poses a great threat to governance but also call for new methods of cyber-security. A high level of public-private partnership is required to address the growing cyber-threats. One of the most critical things in public-private partnership is preparation and commitment from both industry leadership and government (Carr, 2016). It is inevitable for industry to collaborate with government in order to prepare cybersecurity response plans. The security approach of an industry may vary as per the circumstances, however, when systematic abilities are combined with situational awareness operational management for cybersecurity could become a lot easier (Carr, 2016).

# References

Carr, M. (2016). Public–private partnerships in national cyber-security strategies. *International Affairs*, *92*(1), 43–62.

Kuhl, M. E., Kistner, J., Costantini, K., & Sudit, M. (2007). Cyber attack modeling and simulation for network security analysis. *Proceedings of the 39th Conference on Winter Simulation: 40 Years! The Best Is yet to Come*, 1180–1188. IEEE Press.

Rees, L. P., Deane, J. K., Rakes, T. R., & Baker, W. H. (2011). Decision support for Cybersecurity risk planning. *Decision Support Systems*, *51*(3), 493–505.

Rowe, B. R., & Gallaher, M. P. (2006). Private sector cyber security investment strategies: An empirical analysis. *The Fifth Workshop on the Economics of Information Security (WEIS06)*.

Sandoval, J. E., Sapankevych, N. I., Santos, A. J., & Hassell, S. P. (2013). *Cyber attack analysis*.