REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No. 1 (2024)
http://www.veterinaria.org
Article Received: Revised: Accepted:

Beyond Traditional Security: A Defense Analysis of Modern Cyber Threats

Partha Shankar Nayak[1*],Dipankar Basu[2] ,Ranjan Banerjee[3]

[1*]Assistant Professor , Computer Science and Engineering, Brainware University , psn.cse@brainwareuniversity.ac.in
[2]Assistant Professor , Computer Science and Engineering, Guru Nanak Institute of Technology
, dipankarbasu89@gmail.com
[3]Assistant Professor, Computer Science and Engineering, Brainware University, rnb.cse@brainwareuniversity.ac.in

Abstract
As technology evolves, cyber security has become paramount for organizations to meet the needs of all stakeholders. Building both resilience and trust is crucial in protecting against online threats like hacking and identity theft. Security analysts play a critical role in identifying and mitigating cyber threats by analyzing vast amounts of data, including intrusion alerts and network logs. Situation awareness (SA) is essential for developing proactive defense strategies that can disrupt attackers' attempts to penetrate information systems and cause significant harm to organizations.

Keywords: Cyber bullying, Network Security, Cyber-Threat, Situation Awareness, Cyber Defense, Cyber Ethics

Cyber Defense: An Introduction

Cyber defense encompasses network security strategies that focus on preventing, detecting, and responding to various malicious activities, protecting critical infrastructure, and ensuring information security for all organizations within a network. As technology advances, the growing sophistication of cyberattacks makes cyber defense essential for safeguarding assets and maintaining trust and reliability.

Cyber defense techniques involve analyzing potential threats within a given environment to develop effective defense strategies. By identifying and mitigating vulnerabilities, organizations can deter attackers and make it more difficult for them to succeed. Additionally, cyber defense helps optimize resource allocation, improving the efficiency and cost-effectiveness of security measures.

As technology advances and cybercriminals develop more sophisticated tools, traditional network defense methods like firewalls and antivirus software are no longer adequate. These tools rely on static knowledge of existing systems and may struggle to detect emerging threats. By employing threat modeling, attack scenarios, and adversary analysis, organizations can significantly reduce the likelihood of successful cyberattacks and mitigate the risk of data breaches.

To understand how cyberattacks are executed, it is crucial to analyze and gather information about the attack process at every stage. Cyber defense involves various activities aimed at securing organizations, responding swiftly to threats, and continuously improving security strategies.

How could the protection of the data be ensured so that the stakeholders entrust the defense system after Cyber Attack?

Post-cyberattack, safeguarding assets and ensuring business continuity are paramount. Proactive cyber defense strategies are essential to protect sensitive data entrusted by stakeholders. While there's no single solution, effective cyber defense involves protecting critical assets, adapting to evolving threats and regulations, and fostering trust.

Successful cyberattacks often follow a pattern, beginning with reconnaissance to gather information about potential targets. Analyzing these patterns helps organizations better understand and detect threats. A comprehensive defense strategy must address vulnerabilities within the system and protect against both known and unknown threats.

Cyber attackers aim to compromise the confidentiality, integrity, and availability of data, disrupt services, and deny access to resources. They often employ stealthy tactics to avoid detection. In busy networks, the sheer volume of log data can make it challenging to identify potential threats. Security analysts must carefully review and correlate log events to detect anomalies.

Active and Passive Cyber Defense:

Active Cyber Defense

The direct defensive action undertaken to destroy, nullify, or scale back the effectiveness of cyber threats will be explained as Active Cyber Defense. Several in-style security controls use active cyber defenses mechanisms like:

• Blocking users from accessing unauthorized files and alternative resources by Access management mechanism.
• Blocking login tries from adversaries spoofing as legitimate users by passwords and alternative user authentication mechanisms
• Blocking malicious code and packets matching threat signatures or exhibiting abnormal behavior by anti-malware systems, intrusion bar systems (IPSs), and firewalls
• The attacks into isolated systems will be deflected, monitored and unbroken removed from production systems by Honey pots.

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No. 1 (2024)
http://www.veterinaria.org
Article Received: Revised: Accepted:

Passive Cyber Defense
They specialize in creating the measures taken to attenuate the effectiveness of cyber threat against the assets and resources of a corporation. Passive cyber defenses include:
• Cryptography (conjointly referred to as "Secret Writing")
• Steganography (conjointly referred to as "Covered Writing")
• Security Engineering and Verification
• Configuration watching and Management
• Vulnerability Assessment and Mitigation,
• Risk assessment
• Backup and recovery of lost information

Intrusion detection systems (IDSs) area unit primarily passive, however become active after they incorporate components to abort detected threats, morphing into IPSs.

Situation Awareness (SA) for cyber defense:
It is the perception of the elements in the environment within a volume of time and space, the conceptual understanding of their meaning and the projection of their status in the near future. The dream system is one that can self-aware and self-protect itself without employing any humans in the loop, but still it is not completely achieved and is in the stage of research and analysis. Situation Awareness (SA) is achieved by a system which is usually the threatening by random or organized well planned cyber-attacks that the system receives.
The SA systems rely on cyber sensors such as log file sensors, anti-virus systems, malware detectors, and firewalls; they all produce events at a higher level of abstraction than raw network packets that aware a decision maker of a situation till the decision is made. Planning and execution can be done once the decision is made.

Some approaches to gain Situation Awareness (SA) are:
- Vulnerability analysis using attack graphs
- Intrusion detection and alert correlation
- Attack trend analysis,
- Causality analysis
- Forensics (e.g., backtracking intrusions)
- Information flow analysis
- Damage assessment using dependency graphs
- Intrusion response

Some aspects of Situation Awareness (SA) for cyber defense are enumerated below:
1. **Situation Perception**: This aspect includes both identification and recognition of the situation. Intrusion Detection System; an undistinguished part is basically only a sensor that simply identifies an event that may be part of an attack but neither identifies nor recognizes an attack.
2. **Impact Assessment**: There are some aspects to impact assessment:
- Damage assessment or Current Impact assessment
- Future impact assessment (also involves Threat Assessment)
- Vulnerability analysis
3. **Situation tracking**: Keeps track of how situation evolves
4. **Actor or Adversary behavior**: Here, attack trend and intent analysis is taken care of, which are more aligned towards the behaviors of an adversary or actor(s) within a situation than with the situation itself.
5. **Current situation causes (how and why)**: This aspect involves causality analysis and forensics.
6. **Trustworthiness and Quality of the collected situation**: It can also be treated as part of situation perception or more specifically recognition. The quality metrics include truthfulness, completeness and freshness.
7. **Assess probable futures of the current situation**: This involves a group of technologies for projecting future possible actions/activities of an attacker, paths the attacker might take, and then constraining the possible futures into those that are plausible. This drive requires an understanding of attacker's intention and capability.

The below-mentioned aspect is typically not included in Cyber Security Awareness (SA) but still it complements with the above-mentioned aspects in attaining the overall goal of cyber defense.
• **Planning**: This involves identification of better response plans and actions. It is in between the boundary between situation awareness and situation response during which the planned course of action will be taken that involves estimating the effects of a response plan before the planned actions are taken.

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No. 1 (2024)
http://www.veterinaria.org
Article Received: Revised: Accepted:

Cyber Kill Chain
The path followed by an intruder to penetrate information systems over time to develop incident response and analyze capabilities to execute an attack on the victim can be described by a model termed as Cyber kill chain resulting in remarkable disruptive effects on organisations. It is an intrusion-centric model that was the base of cyber security and has been widely used by the security community to describe the different stages of cyber-attacks but for pro-active network defense an early-stage detection of cyber threats is critical to protect against data, financial and reputation loss that could be caused by large-scale security breach.

The General Cyber Intrusion Kill Chain is comprised of the following stages:
- **Reconnaissance**: In this stage, the attacker does research about the targeted system's structures, capabilities, vulnerabilities, etc, i.e, gathers information about the target;
- **Weaponization**: Here, the attacker creates an exploit and malicious payload to send to the target.
- **Delivery**: The attacker sends the exploit and malicious payload to the target through a pre-prepared attack vector like e-mail or other methods.
- **Exploitation**: The execution of the exploit is done.
- **Installation**: In this stage Malwares and Trojan horse in the target system(s) are installed.
- **Command and Control**: Within the victim system, remote control of the infected target device is established.
- **Actions on Objective**: The adversaries perform malicious actions or execute additional attacks on other devices from within the network and the right action is taken to achieve the objectives by working through the kill chain stages again.

To put defensive obstacles, network security defenses are designed to prevent the loss of data and assets.

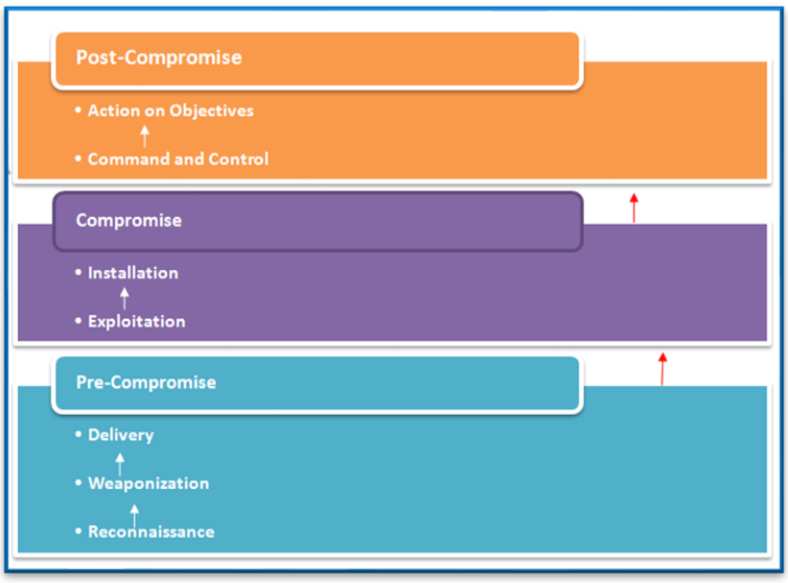

Figure: Cyber Kill Chain Phases

Cyber drills:
At all levels in the organization, the following are enabled by Cyber drills to improve:
- Information & Cybersecurity
- Decision-making capability in Information & Cybersecurity scenarios
- Organizational IT security strategy
- Response to security incidents

To prevent a cyber-attack all possible steps should be undertaken by an organization which could include the best possible technologies with process controls; an attack may still be successful but it always prepares to face and encounter such events. With improved technologies and advancements, the organizations become increasingly connected and their risk for cyber breaches shrouds the risk of other cost related events like natural disasters and fires.

What's more, the personal risk increases for executives and leaders who are ultimately being held responsible for protecting their organization's data (remember Equifax and Uber?). Most organisations fail to strengthen their reactive controls and mostly concentrate only on the preventive and detective controls. Cyber security risks or their resilience

plans are not considered by most business continuity and disaster-recovery plans and organisations need to evaluate if their staff is capable and trained to respond to a cyber incident. Periodical evaluation should be initiated by the organizations to check their cyber incident response capabilities and this can happen through mock cyber war drills or simulation exercises.

Conclusion

The effective defense of information infrastructures will need a blend of both novel strategies and sophisticated technologies. To create efficient defensive plans in order to achieve the full benefit, conceptually clear understanding of the format, security context of each data log and the environment is necessary and it is important to pay attention and establish some initial foundations but challenges are still coming from all corners within its systems and from outside. The task of cyber security defense, on both the individual and team level, is complex, cognitively demanding and often overwhelming, also, let's not forget that attackers are equipped with Artificial Intelligence and Machine Learning powers as well, and systems can be built to predict the behaviors of the models.

References

1. H. Gardner, The Mind's New Science: A History of the Cognitive Revolution, Basic Books,1987.
2. D. Geer Jr., K. S. Hoo, A. Jaquith, "Information security: Why the future belongs to thequants," IEEE Security & Privacy, 2003.
3. C. Sutton, A. McCallum, "Piecewise Training for Structured Prediction," Machine Learning To appear.
4. Alperovitch, Dmitri. (2011). Revealed: Operation Shady Rat. [White Paper]. Retrieved from: http://www.mcafee.com/us/resources/white- papers/wp-operation-shady-rat.pdf
5. Department of Defense. (2011). Department of Defense Strategy for Operating in Cyberspace. Retrieved from: http://www.defense.gov/news/d20110714cyber.pdf
6. McNeese, M., Cooke, N.J., Champion, M.A. (2011) Situating Cyber Situation Awareness. Proceedings of the 10th International Conference on Naturalistic Decision Making.
7. Zetter, K. (2011b) 'FBI vs. Core flood Botnet: Round 1 Goes to the Feds,' Wired, April
8. 26 http://www.wired.com/threatlevel/2011/04/coreflood_results/ (accessed November27, 2012).
9. McGraw, G. (2013) '" Active Defense" is Irresponsible,' Digital blog, February 14. http://www.cigital.com/justice-league-blog/2013/02/14/active-defense-is-irresponsible/ (accessed October 8, 2013).
10. https://www.accenture.com/us-en/services/security/cyber-defense
11. https://en.wikipedia.org/wiki/Proactive_cyber_defense