A Survey of Cyber Security Systems: Approaches for Attack Detection, Prediction, and Prevention

Vera Oliveira

Lusófona University of Porto, Portugal
a21801187@mso365.ulp.pt

Abstract. Nowadays, cyber security is a daily part of life for organizations, governments and the general public of all ages throughout the world. A firm with weak cyber security imposes negative externalities on its customers, employees, and other firms tied to it through partnerships and supply chain relations. Due to the difficulty of identifying and punishing malicious actors, and the ever-greater interconnectedness stemming from the intensified use of the Internet, malicious cyber activity is becoming more and more widespread. One of the main points of it is the globalization and human that factor have become essential to the cyber security proper use and application policies. To this effect, this paper presents a survey of cyber security approaches on the three major topics, attack detection, prediction, and prevention. This paper also reviews the methodologies, strengths, and weaknesses for these approaches. Furthermore, this paper will help predict future cyber attacks and help with preventing from happening again.

Keywords: Cyber Security, Cyber attack, Cyber attack Detection, Security, Threats, Prediction, Prevention, Countermeasure

1 Introduction

The existing approach to cyber security has been mostly reactive. For example, traditional mechanisms to defend against malware are based on matching attacks against known signatures. As new strains of malware are discovered, signatures are added to the list of known attacks. This approach works only if the volume and variety of attacks are low. With the increase in the number of attacks, however, by the time a new attack has been identified, significant damage may already have been done. [1] One of the most problematic elements of cyber security is the quick and constant evolving of cyber risks. Therefore, this paper will help gain an understanding of the threat, explain it and shed some light on how to detect, predict and prevent from one.

10.11228/dpsc.02.01.003

2 Cyber Attack

Cyber attack is the action that attempts to bypass the security mechanisms of computer systems. So, they are any set of actions that threatens the integrity, availability, and confidentiality of network resources. [2]

It's a malicious and deliberate attempt by an individual or organization to breach the information system of another individual or organization. Usually, the attacker seeks to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of anything that has value to the organization or individual. [3]

Cybercrime has increased every year as people try to benefit from vulnerable business systems. Cyber threats can also be launched with ulterior motives. Some attackers look to obliterate systems and data as a form of "hacktivism". [4]

Cyber security concerns with the understanding of the surrounding issues of diverse cyber attacks and devising defense strategies that can preserve confidentiality, integrity, and availability of any kind of digital and information technologies. [5]

2.1 Purpose and Motivations

Sometimes we ask what motivates cyber attackers, and why they do it. Understanding the motives behind a targeted attack is important because it can help pinpoint what to protect and how to protect it. A simple profit motive scenario can be a smokescreen hiding a different, deeper kind of attack, such as:

Espionage: usually aimed at gathering information from the victim. It's a clandestine activity and the attackers strive to avoid detection, at least until they achieve their goal. These are also among the most persistent often continuing the attack vector even after they've been detected.

Profit: direct financial gain a common profit-driven attack in use today and include theft and resale of credit card information or ransomware.

Ideological: someone that wants to harm the reputation, deny services to customers, or sabotage the systems to further their propose or eliminate perceived threats to the environment, for example, a frustrated ex-employee.

Information Theft: when the aim is to acquire information owned by the target and/or stored in the network. This information can be in form of customer information, business-critical information or even intellectual property.

Several others self-explanatory purposes for example extortion, revenge or sabotage. [6]

2.2 Common types of cyber attacks

Malware: is a term used to describe malicious software, that breaches a network through a vulnerability, most typically when a user clicks on a dangerous link or email with an attachment that will lead to risky software installation. Once inside the system, the malware can disrupt certain components of the network and block the access to the system, it can also obtain information by transmitting data from the hard drive or installing additional harmful software.

Phishing: is the practice that gathers sensitive information like login credentials, credit card numbers, bank account numbers or other financial information by masquerading itself as a legitimate site. This type of scams creates a sense of urgency to manipulate users. [7]

Denial-of-service (DoS): it floods the systems, servers or networks with traffic to exhaust resources and bandwidth. As a result, the system is unable to fulfill legitimate requests or simply crashes.

Man-in-the-middle attack: also known as eavesdropping attack, occur when an attacker inserts themselves into a two-party transaction. Once in the middle, they can access, read and change secret information without keeping any trace of manipulation. [8]

Brute force attack: comprises repeated attempts to gain access to protected information until the correct key is found, for example, passwords.

Social engineering: is the technique used to gain unauthorized access to information through human interaction, also known as human hacking. Engebretson [9] defines social engineering as "one of the simplest methods to gather information about a target through the process of exploiting a human weakness that is inherent to every organization." The attack aims at manipulating victims to divulge confidential information.

Furthermore, there are two types of attacks scenario:

Un-targeted attacks: which attackers indiscriminately target as many devices, services or users as possible. The attacker doesn't care about the victim is as there will be several targets.

Targeted attacks: the attacker has a specific interest in your business or has been paid to target you. A targeted attack can often be more damaging than un-targeted one because it has been specifically tailored to attack your systems, processes or personnel, in the office or at home. [10]

3 Cyber Attack Detection

Cyber attack detection is a common attack mitigation technique. It involves responding to an abnormal connection to report the presence of an attack pattern or profile in a network. With the ever-increasing threat environment, no matter what level of protection a system may have, it will get compromised given a greater level of motivation and skill. A defense in layers strategy should be deployed so when each layer fails, it fails safely to a known state and sounds an alarm. The most important element of this strategy is timely detection and notification of a compromise. Intrusion detection systems (IDS) are utilized for this purpose, it is the process of identifying an intrusion or attack signature in a continuous flow of connections. [11]

3.1 Analysis Approach

Currently there are three basic approaches to cyber attack detection, mostly used to make the engine analysis by processing the data in order to identify cyber attacks.

Misuse Detection: misuse detectors analyze system activity, looking for events or sets of events that match a predefined pattern of events that describe a known attack. This approach is concerned with finding intruders who are attempting to break into a system by exploiting some known vulnerabilities. The basic idea is to use the knowledge of known attack patterns and apply this to identify attacks in various sources of data being monitored. Therefore, the efficacy of the system relies heavily on the thorough and correct construction of this knowledge base.

Anomaly Detection: is the identification of rare items, events that raise suspicions by differing significantly from the majority of the data. [12] Anomalous data can indicate critical incidents, a glitch or an attack.

Specification-based Detection: specification-based approach of misuse detection works just like the existing anti-virus software. [13] The specification-based techniques in this approach are used for reducing the number of false alarms. [14] But they are not as effective as anomaly detection, especially when it comes to network probing and denial-of-service attack.

3.2 Cyber Attack Detection Systems

Cyber Attack Detection Systems (CADS) is a software that automates the process and detects possible cyber attacks. They have three major security functions: monitor, detect and respond to unauthorized activity by company insiders and outsiders attackers.

Antivirus Software: is a computer software used to detect, identify, prevent and remove malicious software. [15] This type of programs is not always effective against

new viruses, the reason is that before releasing them, the virus designers test them on the major antivirus applications.

Firewalls: is a network security system for monitoring and control over the incoming and outgoing network traffic based on predetermined security rules. [16] A firewall typically establishes a barrier between a trusted, secure internal network and another external network, it will filter traffic between these two and controls network traffic in and out of that single machine. The attempt to bypass the firewall rules may result in the creation of an open channel for attackers to attack. [15]

Haystack: it was developed for the detection of cyber attacks in multi-user Air Forge computer system. To detect cyber attacks the system employs two methods of detection anomaly detection and signature-based detection. [17]

Later haystack was implemented on an Oracle database management system running on an IBM-AT clone. Haystack periodically downloaded the audit trail file from the target Standard Base Level Computers (SBLC), this file contained the session duration, number of files opened, number of pages printed, number of CPU resources consumed in the session, and number of sub-processes created in the session. In total, the system included more than 30 features for each session because there was no notion at the time of which feature were most effective in detection intrusions. [18]

MIDAS: although old, Multi Intrusion Detection and Alerting System (MIDAS) was designed and written to perform rule-based cyber attack detection. For developing, compiling, and debugging the rules. [19] It was designed to take data from Docmaste's answering system audit log. This data was organized, used to construct session profiles, and then compared to user profiles of normal behaviour. MIDAS combined statistical anomaly detection with expert system rule-based approaches. [18]

IDS: is a device or software application that monitors and analyse a network or system for signs that malicious activity are taking place to either infiltrate or steal data from the network. IDS compares the current network activity to a known threat database to detect the kind of behaviour like security policy violations, malware, and port scanners. IDS requires a human or system to verify the results to determine what actions to take next.

4 Cyber Attack Prediction

To predict the future, you are restricted to examining the past. Any event can be predictable if it occurs in a non-random way, allowing to extract random contexts that may be based on learning and identifying associations. Prediction comprises two types of activities: on one hand, forecasting or prediction in the narrow sense, and anticipation on the other. The key distinction between both is that in the former, current actions are

based on past behaviour, while in the latter, predictions about the future guide current actions. With this anticipatory processing, benefits include an increase in accuracy, speed or maintenance of information processing. [20]

4.1 Predictive analytics and machine learning

Predictive analytics is the art of building and using models that make predictions based on patterns extracted from historical data. Some peculiarities of cyber security also make it more challenging to apply machine learning and the evolution of attacks that requires learning to be incremental. Machine learning is often used to build predictive models for classification and to cluster data, this technique can be grouped into supervised, unsupervised, and hybrid techniques.

One of the challenges in cyber security context is that machine learning models can themselves be attacked. [21] Through a carefully attacks, attackers can gain an understanding of the internal state of a machine learning model, which allows them to attack more effectively in the future.

4.2 Vulnerability prediction

In other words, vulnerabilities are weaknesses, flaws that can be exploited by threats to cause harm to an asset. Given that not all vulnerabilities are of equal impact and if resources are limited, the manager needs to prioritize on which patches to create or to deploy. Vulnerability prediction can be of assistance in this task by predicting the kinds of vulnerabilities that exist in a system and the risk of them being exploited. One way to know almost all the vulnerabilities that exists is to use NVD, that is the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP). [22]

4.3 Honey Implementation

Honeypot is a computer security mechanism set to detect, deflect, or counter the attempts at unauthorized system. Generally, a honeypot consists of data, and it appears to be a piece of real information and it would be in a part of the system but actually isolated and monetarized, as it seems to contain resources or value information to the attackers, it attracts their attention.

Two or more honeypots on a network form a honeynet. They are used for monitoring a larger and more diverse network. [23]

5 Cyber Attack Prevention

Prevention of attacks is a proactive activity that identifies and responds to potential threats in a network quickly. Most detection approaches are reactive and are only applied after much damage has been done on the impact zone. Several intrusion prevention systems (IPSs) have been proposed as a tool for improving cyberspace security. Cybernetic prevention has the primal act of restricting, controlling, removing or preventing the occurrence of cyber attacks in a computer system. Cyber prevention is responsible for detecting irregularities in the activities of the Internet user. [24]

IPS: an Intrusion Prevention System live in the same area of the network as a firewall, between the outside world and internal network. this proactively deny network traffic based on a security profile created if that packet represents a threat it will be dropped before, they reach their target. Just like IDS, it requires that the database gets regularly updated with new data threats.

Prevention Tips: falling victim to cyberattacks can be devastating, it causes downtime, the damaged reputation of the firm. Aside from the more conventional solutions, like the anti-virus and the firewall, there are simple, economical steps to reduce the risk:

1. Train employees in cyber security principles.
2. Make backup copies of important data and information.
3. Control physical access to your computers and network components.
4. Limit employee access to data and information and limit authority to install software.
5. Regularly change passwords.
6. Require individual user accounts for each employee.
7. Regularly update antivirus and antispyware software and applications as they become available.

6 Detecting and Defending against Phishing attacks

One of the most persistent security challenges is phishing. This is true for both organizations and individuals. Whether gaining access to credit card information, security passwords, or any other sensitive information, hackers can use different techniques, such as social engineering, emails, phone calls, and other forms of communication, to steal data. This opens businesses as worthwhile targets since they have valuable data on hand. Evidence that it is necessary to include the human factor in security modelling. These are attacks in which, typically, the victim is deceived to give out secret information enabling access to a given resource [25]

8

6.1 Common way of cyber criminal attacks

- Sending a link through email that opens a malicious website.
- Placing a trojan in the target's computer through an email attachment.
- Creating a spoofed email to look as reputable as possible and tricking the receiver.
- Impersonating a vendor or IT department and calling via phone.
- A technique where content with malicious intent is injected into the company's website to obtain passwords.
- Hackers positioning themselves in the middle of the company and their customers to capture any and all information transmitted between them.
- DNS-based phishing attack that forces people into a malicious website when they try to visit the target website.

6.2 How to defend against phishing attacks

- Use an SSL certificate on your website to protect all information transmitted between the web server and the visitor's browser.
- Provide proper and regular training to employees about phishing, how to identify it, and what to do when they suspect an attack.
- Ensure that all security tools, protocols, and controls are up to date. Also, take note of new developments in the IT industry about tools and new types of attacks, to be able to adapt to the company's defenses.
- When a payment page is needed for your website, make sure to use a securely hosted page. This is the best practice in order to secure credit card information being transmitted over the internet.
- Create a filter that can detect the most common types of spam and phishing attacks. This should be also able to identify attachments and filter malicious ones.
- Use an antivirus solution for each endpoint device, as well as the entire network.
- Encrypt the sensitive data of the company so they are difficult to open even when stolen.
- Use a web filter in order to block malicious websites from even opening on your network.
- Disable HTML email feature within the organization, which will reduce the risks of phishing attacks.
- Make sure to require proper encryption for all employees who telecommute or work remotely.

10.11228/dpsc.02.01.003

7 Conclusion

Despite all the efforts that have been done in the last three decades to prevent widespread dissemination of insecurity in the Internet traffic by the most important companies (Kaspersky, Microsoft, Symantec, among others), the battle is yet to be won. Reading their monthly newsletters gives us an accurate idea of the huge challenge they're facing today. The rate of solved security threats every month is much lower than the patches they send their customers to "remain secure" today. The main idea prevailing is "You remain secure until you press the ENTER key" or "LOG IN" in an internet URL.

References

1. Michael Weiss.: From prediction to anticipation of cyber attacks. IJBT (2018).
2. Shailendra Singh and Sanjay Silakari.: A Survey of Cyber Attack Detection Systems. In: International Journal of Computer Science and Network Security, VOL.9 No.5, (2009).
3. INTERNATIONAL STANDARD.: ISO/IEC 27000:2009(E).
4. What Are the Most Common Cyber Attacks https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html, last accessed 2019/12/15.
5. Julian Jang-Jaccard, Surya Nepal.: A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, 80 (2014).
6. Know your cyber enemy by IBM Security, https://www.ibm.com/downloads/cas/ZDEYR18P, last accessed 2019/12/17.
7. Andreea Bendovschi.: Cyber-Attacks – Trends, Patterns and Security Countermeasures. Elsevier (2015).
8. Avijit Mallika, Abid Ahsanb, Mhia Md. Zaglul Shahadata and Jia-Chi Tsouc.: Man-in-the-middle-attack: Understanding in simple words. International Journal of Data and Network Science (2019).
9. Engebretson P.: The basics of hacking and penetration testing: ethical hacking and penetration testing made easy. Elsevier (2011).
10. Great Britain, Government Communications Headquarters, Computer Emergency Response Team UK.: Common Cyber Attacks: Reducing The Impact. BIS (2015).
11. N. B. Aissa, M. Guerroumi.: "Semi-supervised statistical approach for network anomaly detection". Procedia Computer Science, (2016).
12. Zimek, Arthur, Schubert, Erich.: "Outlier Detection". Encyclopedia of Database Systems, Springer New York, (2017).
13. Jamal Raiyn.: A survey of Cyber Attack Detection Strategies. International Journal of Security and Its Applications Vol.8, No.1 (2014).
14. R. Sekar, A. Gupta, J. Frullo, T. Shanbhag, A. Tiwari, H. Yang, S. Zhou.: "Specification-based anomaly detection: a new approach for detecting

network intrusions". In: Proceedings of the 9th ACM conference on Computer and communication security, pp. 265– 274, Washington D.C., USA, (2002).
15. Martellini, Maurizio, Malizia, Andrea.: Cyber and Chemical, Biological, Radiological, Nuclear, Explosives Challenges: Threats and Counter Efforts. Springer. (2017).
16. Todd Lammle.: CCNA Routing and Switching. Complete Review Guide. John Wiley & Sons, (2016).
17. Stephen E. Smaha. Haystack: An intrusion detection system. In proceedings of the IEEE Fourth Aerospace Computer Security Applications Conference, Orlando, FL, USA, (1988).
18. Rebecca Gurley Bace.: Intrusion Detection.1st edn. Sams Publishing. Indianapolis, (2000).
19. Michael M. Sebring, Eric Shellhouse, Mary E. Hanna, R. Alan Whitehurst.: Expert systems in intrusion detection: A case study. In: Proceedings of the 11th National Computer Security Conference, pages 74.81, Baltimore, Maryland, (1988).
20. Andreja Bubic, D. Yves von Cramon, Ricarda I. Schubotz.: Prediction, Cognition and the Brain. Front Hum Neurosci, (2010).
21. Barreno, M, Nelson, B, Joseph, AD, Tygar.: JD: The security of machine learning. Machine Learning, 81, pp. 121–148 (2010).
22. National Vulnerability Database, https://nvd.nist.gov/#, last accessed 2019/12/17.
23. Mr.S.Thanigasalam, Dr.M.Savitha Devi.:Finding Attackers Details to Solve Security Issues Using Honeypots Technique. Shanlax International Journal of Arts, Science and Humanities (2018).
24. Valdemar Sousa.: A Review on Cyber Attacks and Its Preventive Measures. Proceedings of the Digital Privacy and Security Conference (2019).
25. Markus Jakobsson.: Modeling and Preventing Phishing Attacks. Financial Cryptography, (2005).