JOUN TECHNOLOGIES

Cyber Security Fundamentals in Business Enterprises

Ethan Sanchez

Abstract

As businesses transition to digital-centric operations, reliance on interconnected networks escalates, underscoring the critical importance of cybersecurity. The advent of innovative technologies brings forth new threats, vulnerabilities, and risks, challenging enterprises across all sectors. Establishing a robust security foundation becomes imperative to safeguard organizational assets effectively. This paper aims to delve into the multifaceted realm of cybersecurity, spanning foundational concepts, contemporary practices, and future trends, to equip businesses with insights and strategies to navigate the evolving cybersecurity landscape.

 ©2024 Joun Technologies

Table of Contents

Introduction

As businesses evolve, they start to rely more on digital technologies and interconnected networks. Because of this, the importance of cyber security cannot be overstated. With cutting edge technologies starting to develop for businesses to use, more threats, vulnerabilities, and risks also start to form along with it, which is a landscape that challenges businesses across all industries. To protect an organization and their assets, they must prioritize an effective foundation of security.

Cyber Security Terms and Practices

There are three major exploits in a business's security: threats, attacks, and vulnerabilities. A threat is referred to as any potential danger that can exploit a vulnerability in a system or network. They can come externally or internally in a business such as unaware employees, natural disasters, or data breaches. An attack is the actual exploitation or malicious action that is carried out in the system or network by leveraging a threat. It can be described as malware infections, phishing attacks, ransomware, or social engineering. Lastly, a vulnerability is a weakness or flaw in software, hardware, configurations, or processes that can be exploited by attackers to compromise the business's security. Some common examples of this include using an old version of software, weak passwords, or misconfigured access controls. The strength of an organization's cyber security is called the [3] "Security Posture" and is defined as how well they can predict, respond, and prevent exploits.

 ©2024 Joun Technologies

To prevent these exploits, business professionals must know the CIA triad which is a foundational concept in information security. It stands for Confidentiality, Integrity, and Availability. These principles are the basis for designing and implementing security controls to protect company assets. Confidentiality means ensuring the sensitive information is accessible to the right people or entities and to prevent unwanted disclosure to those who should not see it. Integrity is about maintaining accuracy, consistency, and trustworthiness of data by preventing alterations or tampering. Availability is about ensuring access to data so that business operations can be fulfilled while managing impacts from disruptions or outages.

History of Cyber Security Practices

The rapid evolution of digital technologies has driven many changes in security practices and implementations. The legacy of cyber security spans decades of innovation, challenges, and historical milestones. Some of the best examples include security frameworks, encryption, firewalls, and vulnerability management.

To build a strong foundation, security frameworks are created and followed so that regulations and policies are met by businesses. Security frameworks establish guidelines, best practices, and standards for organizations to establish, implement, and improve their security posture. The most known cyber security framework is the National Institute of Standards and Technology or NIST Cyber security framework. [7] The NIST framework recently updated to 2.0 on February 26, 2024, which has been the first major update since its creation in 2014. Other known frameworks include the ISO/IEC 27001, CIS Controls, and COBIT, all of which offer a systematic approach to risk management, security controls, compliance, and continuous improvement to help organizations align their security in the right direction to industry standards and regulations.

How Attacks and Defense have changed over the years

Over the years, businesses have encountered many different cyber-attacks compromising their assets. Because of these attacks, the security foundation and structure in current companies has changed to better protect themselves. Unfortunately, as defenses become stronger, hackers try to pry into whatever vulnerabilities they can find in a business. It is a vicious cycle that will forever be changing and growing; however, it is important to learn about some of the most infamous attacks and famous countermeasures that have taken place over the years to recognize how to prevent similar occurrences happening to businesses today.

©2024 Joun Technologies

All industries have some form of valuable information; therefore, breaches occur in all industries. For example, [5] Target was a victim in 2013 where phishing emails on third party contractors were used to infiltrate Target's network. From there, the threat actor was able to infect Target's point-of-sale systems with malicious software. Finally, once the threat actor distributed the malware to enough systems, they launched the malware and began to collect customer data. Although the third-party contractor, Fazio Mechanical, failed to detect the malware, Target was able to notice the vulnerabilities with their security software provided by FireEye. This attack required the assistance of many government players such as the US Department of Justice, the Secret Service, and the FBI. [10] The result of this attack was that the cyber criminals were able to compromise around 40 million customers' credit and debit card information as well as 70 million customers' personal details. Ultimately, the Payment Card Industry Data Security Standard (PCI DSS) had to go through revisions following this attack which mainly targeted third-party security. These revisions included enhanced encryption requirements, stricter access control measures, improved monitoring, and logging, and regular security training.

The nature of phishing attacks has changed. According to [8] Merilyn Stuck, a professional in cyber solutions, one of security's biggest threats isn't from malicious software or lack of encryption but from people themselves. [9] With the proper social engineering to the right people, hackers can gain access to whole infrastructures as a result.

Social engineering is the mechanism for malicious attempts being accomplished through human interactions. Psychological manipulation is used to produce security mistakes like sharing sensitive information. [6] In 2023, Caesars Entertainment was attacked through social engineering which led to the theft of data from members of their customer rewards program. Again, in similar fashion to the Target breach, a third party was abused to gain access to the main victim's data; this time it was an IT support vendor that worked with Caesars Entertainment. The hacker group ScatteredSpider stole Social Security numbers and driver's license numbers from the members. In this case, the security solution that Caesars Entertainment decided on was to pay out the $30 million ransom that the hacker group demanded. Sometimes, paying the ransom ends up being the most efficient solution with respect to response time and resources needed for countermeasures.

The Importance of Information Security

Information security is more than just safeguarding data. Cyber and information security represents a critical importance for organizations to ensure business continuity, customer trust, and maintaining a competitive advantage. Some share the opinion that because one cannot see the profits a security center brings it is just a mere cost center. Understanding the broader implications of information security, business professionals now recognize the strategic value and invest in robust security measures that safeguard assets and build the brand's reputation as we move further into a digital world.

Valuing and viewing cyber security throughout a business or organization is easier understood when seen less of an afterthought and more of a proactive measure. Many examples lead to this; critical infrastructure like the healthcare industry can be secured against attacks so that devices keeping patients alive stay working or in the telecommunications sector where it plays a critical role in facilitating communication for those in emergency situations. [2] "The

cost to operate is much lower than the damages and impact" is a quote from a blue team detection professional interviewee. Developing and implementing preventative measures will save more money and assets over the cost comparison of repairing the damages of a cyber-attack.

Types of Attacks that companies currently face

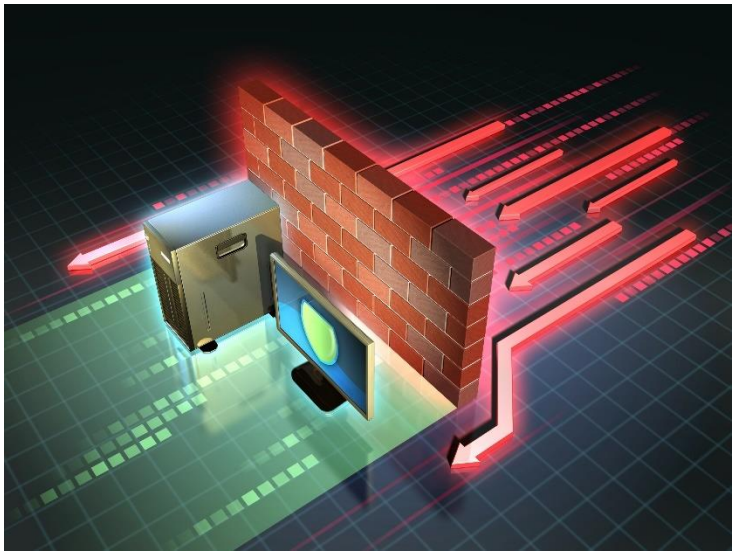
Companies face a myriad of sophisticated attacks that exploit vulnerabilities in their digital and physical infrastructure and operations. These attacks can come from malicious emails, ransomware, or even unaware employees. And as technology advances, so do attacks, which is why it's important to know the types of attacks that are currently being used on companies today. By understanding the nature and prevalence of these attacks, businesses can prepare their security defenses against these threats in this cyber security landscape.

As the development of artificial intelligence emerges, so do its vulnerabilities. AI is one of the most rapidly evolving technologies that is in a sweet spot for gathering generational and young talents to its field. A Chevy dealership in Watsonville California took advantage of a chatbot, powered by ChatGPT AI, to respond to customers. This was quickly discovered and was exploited by several users. A user manipulated the chatbot with tricky wordplay to legally sell him a Chevy Tahoe for $1 dollar. The offer was eventually rejected but it showed the security risks associated with turning over control to AI systems.

©2024 Joun Technologies

Ways Companies can defend themselves from Threats, Attacks and Vulnerabilities

Burpsuite, Wireshark, and Nessus are all tools to discover vulnerabilities in a webspace. Tools like these are important to a business's security because they leverage the ability to find the problems in the foundation of the company before malicious users do. Simple firewalls for a



company's network can reduce the possibility of having an employee accidentally click a malicious link. Firewalls in the business setting can allow expected connections into the company's network as well as prevent unexpected intruders from accessing the network space. All businesses and organizations that utilize the internet need some form of firewall, but all vary based on the context. The most advanced firewall available is [1] Next-Generation Firewall (NGFW) and is the future of network security. This updated firewall adds functions such as malware and virus scanning as well as a simple design allowing security teams to control the system from a single application, including the delivery of updates across the entire network.

How Companies implement Different Types of Security Practices

New security practices occur periodically, which can be a double-edged sword to an organization. Organizations need to adapt and recognize the strengths and flaws that current and past security practices yield. For example, at one-point [4] NIST had set the standard to periodically change a user's password to prevent unauthorized access to accounts. Now, NIST favors two factor authentication as the norm for keeping accounts secure. Two factor authentication makes it harder for threat actors who have password cracking capabilities by requiring a second form of identification. On top of requiring the user to authenticate through approval, further measures also include network securities. What this means is that in some cases, an employee is usually expected to log in through the company's internal IP address space, so if a hacker manages to try to log in outside of this space, then security alarms could prevent access. Whether it comes from a user's personal phone, secret numerical code, or biometric security, the standard of two factor authentication has made accounts resilient.

Another common yet extremely effective security practice is security training for employees. As described before, one of the biggest security concerns is an individual, so to combat this, internal security training is one of the best counter measures to protect assets and data. An employee at the company can give access control to threats actors if manipulated properly. Companies employ "ethical hackers" to find weaknesses and vulnerabilities in a company before a malicious threat actor outside the company does so that it can be improved and fixed. These sorts of preventative measures are what help to prevent companies falling victim to financial losses and disruptions as well as keeping an organization running smoothly on an operational day.

Cyber Security and the Future

In the future of cyber security, we welcome new technologies being developed with open arms. People are developing technologies like artificial intelligence, zero trust architecture, quantum cryptography, and behavioral biometrics which can be leveraged into the daily usage of security. [2] In an interview with a blue team detection professional, he stated his work with endpoint detection response solutions is becoming less strainful for a full stack detection team as the use of AI helps make detecting suspicious activities and monitoring files easier. There is an argument that can be made about how AI can take over the need of human analysts to defend against malicious activity. The accuracy rate of AI is not at a point where it can be entirely relied on as it would risk the integrity of a company's security and reputation.

Concluding thoughts

In the realm of digital technologies and interconnected networks, cyber security as a critical component of business infrastructure cannot be overstated. In worst case scenarios, a fallback plan to keep assets secure, private, and ready for the right people must be in place to continue business operations. A key element of company security is to ensure everyone knows the importance of their role and how they fit into the overall organization's security strategy. Embracing these advancements and adopting proactive security measures, businesses and organizations alike can thrive with security in check.

©2024 Joun Technologies

References Page

[1] *Benefits of firewalls for business*. NordLayer. (n.d.). https://nordlayer.com/learn/firewall/benefits-of-firewall/

[2] Gomez, J. (2024, March 13). Cyber Security in Business . personal.

[3] Hashemi-Pour, C., & Rosencrance, L. (2023, October 3). *What is security posture?: Definition from TechTarget*. Security. https://www.techtarget.com/searchsecurity/definition/security-posture#:~:text=Security%20posture%20refers%20to%20an,respond%20to%20ever%2Dchanging%20cyberthreats.

[4] Hibbert, C., Kriel, K., & Schissel, N. (2023, August 30). *From NIST 1.1 to 2.0: Understanding the evolutions in cybersecurity strategy - MLT Aikins - western Canada's law firm*. MLT Aikins. https://www.mltaikins.com/innovation-data-technology/privacy/from-nist-1-1-to-2-0-understanding-the-evolutions-in-cybersecurity-strategy/

[5] *Inside Target Corp., days after 2013 breach*. Krebs on Security. (2015, September 21). https://krebsonsecurity.com/2015/09/inside-target-corp-days-after-2013-breach/comment-page-1/

[6] Jones, D. (2023, October 9). *Caesars Entertainment says social-engineering attack behind August breach*. Cybersecurity Dive. https://www.cybersecuritydive.com/news/caesars-social-engineering-breach/695995/#:~:text=Caesars%20Entertainment%20confirmed%20that%20a,the%20Maine%20attorney%20general's%20office.

[7] *NIST releases version 2.0 of Landmark Cybersecurity Framework*. NIST. (2024, February 27). https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework

[8] Stuck, M. (2024, February 22). Cyber Security in Business Settings. Personal.

[9] *What is Social Engineering: Attack Techniques & Prevention Methods: Imperva*. Learning Center. (2023, December 20). https://www.imperva.com/learn/application-security/social-engineering-attack/

[10] Young, K. (2021, November 1). *Cyber case study: Target data breach*. CoverLink Insurance - Ohio Insurance Agency. https://coverlink.com/cyber-liability-insurance/target-data-breach/

About the Author

Ethan Sanchez

Ethan Sanchez is a final year Management Information Systems student at California State University of San Marcos. He is defined by his passion for cyber security in the business world and how he can soon help prevent malicious activities to those affected. With the help of Joun Technologies, he wrote this paper in hopes of sharing to unaware individuals about the importance of cyber security in the upcoming digital world.

©2024 Joun Technologies