WEB SECURITY

IN DAY TODAY LIFE

LOVELY PROFESSIONAL UNIVERSITY

Phagwara, Punjab

Submitted by:

VYSHNAV P | 12205220 |B (52) |D2213

Date of submission: 30/11/2022

Vyshnav7675@gmail.com

ACKNOWLEDGEMENT

I hereby solemnly certify that the term paper prepared is based on work completed during Sem I of MCA during Term 1 of 2022 under the guidance of Madam Pallavi Vyas (Asst Prof, LPU). I also certify that the guidelines used in the term paper were provided by the instructor. I'd want to thank ma’am as well. Madam Pallavi Vyas, who practically implanted knowledge within me, allowing me to complete my assignment on time. This paper would not have been a success without the outstanding assistance of my supervisor, Madam Pallavi Vyas.

ABSTRACT

Web apps are one of the most used platforms for delivering information and services via the Internet today. Web applications are becoming a popular and attractive target for security assaults since they are increasingly employed for vital services. Although a vast body of strategies has been established to fortify online applications and prevent web application assaults, little work has been given to connecting these techniques and developing a big picture of web application security research. This study also provides a detailed evaluation of the discussed attacks against selected important parameters. Similarly, observational data about Email-based assaults over an unspecified time period is shown. The report concludes by highlighting the significance of such studies and research possibilities in this area.

Keywords: Firewall, Password, file permissions, SSH

1. INTRODUCTION

Understanding web security is critical if you want to safeguard your website, data, and company in general. It will be much easier to defend yourself and avoid difficulties once you grasp the obstacles that might develop in the area of web security. There will always be hurdles in business, but if you execute it well, nothing is impossible. With that in mind, we will discuss Web Security and the benefits it can provide you, as well as all of the potential obstacles it may provide and how you may overcome them.

2. WEB SECURITY DEFINITION

Web security refers to a broad range of security solutions that protect individuals, devices, and larger networks against Internet-based cyber-attacks (virus, phishing, and so on) that can result in security breaches and data loss. Many online security solutions lower your organization's security risk if a person encounters a harmful file or website by accident.

A "stack" of security devices at the Internet gateway inspects traffic as it passes through under the traditional online security approach. This comprises firewall inspection, intrusion prevention system (IPS) scanning, sandboxing, URL filtering, and a variety of additional security and access control combinations.

3. WHAT IS THE PURPOSE OF WEB SECURITY?

It is a critical aspect in attaining consistency. It is your first line of protection against attacks that might reveal sensitive data, demand large ransoms, cause reputational harm, violate compliance, and have a variety of other implications.

Cyber dangers, formerly the domain of amateur hackers, have developed into a vast black-market enterprise, affecting organized crime, state-sponsored espionage, and sabotage. Some of the most recent dangers are quite clever, readily fooling the inexperienced and evading obsolete security systems. A plethora of commercial tools, exploit kits, JavaScript plugins, and even full-fledged campaigns make it simple for unskilled attackers to initiate attacks.

4. WHAT ARE THE BENEFITS OF WEB SECURITY?

For modern enterprises, effective online security provides several technological and human benefits.

- By safeguarding their personal information, we can protect both our clients and staff.
- Improves user experience by assisting in keeping users safe and productive.
- Stay safe and out of the press to maintain client loyalty and confidence.

Unfortunately, since it goes both ways, attackers have more chances to approach an organization's wider attack surface. You may spend more time reaping the advantages and less time worrying about security concerns if you have the proper online protections in place.

5. WHAT DOES WEB SECURITY PROTECT?

Web Security employs a diverse network to safeguard users and endpoints against malicious emails, encrypted threats, malicious or hijacked websites and databases, malicious redirection, hijacking, and other attacks. Let's look more closely at some of the most frequent risks.

- ❖ Malware in general: There are several malware variations that cause data breaches, espionage, unauthorized access, bans, flaws, and system failures.
- ❖ Phishing: These assaults are frequently carried out using email, text messaging, or malicious websites in order to fool people into disclosing their login credentials or downloading malware.
- ❖SQL Injection: These attacks take advantage of input flaws in database servers to execute instructions

that allow attackers to retrieve, alter, or destroy data.

- Denial of Service (DoS) attacks can cause network devices such as servers to slow down or even shut down by delivering more data than they can manage.
- A distributed DoS (or DDoS) assault is carried out at the same time by a large number of hijacked machines.
- Cross-Site Scripting (XSS): An attacker injects malicious code into a trustworthy website by inserting malicious code into an unprotected user input field.
- Ransomware: encrypts your data and demands a ransom payment in return for a decryption key. A double extortion assault also steals information.

The optimal online security solution employs a variety of technologies to detect malware and ransomware, block phishing sites, limit credential usage, and develop a comprehensive defense.

6. HOW DOES WEB SECURITY WORK?

Web security features exist between your environment's endpoints and the Internet. From there, monitor traffic and queries in both directions. While no one technology can monitor or audit all traffic, a "stack" of appliances or today's more effective cloud-delivered service platforms can help to prevent policy violations, malware infections, data loss, and credential theft, among other things.

Many solutions are now available, some of which are more thorough than others. Web security technologies include the following in the whole stack:

a) Secure Web Gateway (SWG) protects Internet users from threats and enforces policies to prevent infections and block unwanted traffic.

b) Network security, app management, and visibility are all provided by firewalls/IPS. A cloud firewall, which can be updated and expanded based on your needs and encryption, is a more practical alternative.

c) URL Filter filters and eliminates unwanted traffic and information while also protecting against web-based viruses.

d) The sandbox places software in a safe area where it may be inspected and operated without infecting the system or other applications.

e) Browser Isolation loads a web page or app into a distant browser and delivers just pixels to the user, preventing data or documents from being downloaded, copied, pasted, or printed.

f) DNS Control establishes rules that regulate DNS traffic requests and answers, allowing you to identify and prevent DNS abuse such as tunnelling.

g) Antivirus software identifies and eliminates Trojans, spyware, ransomware, and other malware. Many programs additionally guard against attacks such as malicious URLs, phishing, and distributed denial of service (DDoS).

h) TLS/SSL Decryption divides encrypted communication into inbound and outgoing streams, inspects the content, re-encrypts it, and sends it to its destination.

7. CLOUD-DELIVERED WEB SECURITY CASE

Web security technology is contained in data center SWG equipment as on-premises hardware. To cover all functions, the hardware stack may contain firewalls, URL and DNS filters, sandbox appliances, and so forth.

The issue with hardware-based techniques is the inevitability of a gap. To guard against zero-day attacks, appliances must be patched on a regular basis. Any delay in patching puts vulnerabilities open to attack. Appliances, too, have performance constraints. TLS/SSL-encrypted traffic, in particular, accounts for practically all traffic today. This means that concealed hazards cannot be completely eliminated.

Furthermore, because so many devices (often from the same manufacturer) do not interact with one another, even highly competent information security specialists cannot associate them.

Secure online gateways supplied as cloud services, on the other hand, enable real-time threat prevention and policy enforcement, blocking access to infected websites when users are outside the corporate network. Unwanted traffic should be blocked. From internal network access.

8. CONCLUSION

Web security plays an important role in the realm of data innovation. Data security has proven to be one of the most difficult challenges nowadays. Computer security is a vast issue that is becoming increasingly important as the globe becomes increasingly networked, with systems being used to accomplish simple interactions. With each New Year that passes, digital malfeasance continues to swerve in new directions, as does data security. The most current and troublesome developments, coupled with new digital instruments and risks that emerge on a daily basis, are putting organizations to the test in terms of how they safeguard their foundation, as well as how new phases and understanding are required to accomplish so. There is no ideal solution for digital wrongdoings, but we should do our utmost to restrict them with the final objective of having a safe and secure future on the internet.

9. REFERENCES

1. Professional Development. (2016). Retrieved from https://nicerc.org/pd/

2. Professionalizing the Nation's web security Workforce? Criteria for Decision-Making. (2013). Retrieved from https://www.nap.edu/read/18446/chapter/5

3. Reauthorization of Carl D. Perkins Vocational and Technical Education Act. (2007, March 16). Retrieved from https://www2.ed.gov/policy/sectech/leg/perkins/index.html

4. Recruiting and Retaining Cybersecurity Ninjas. (2016, October 19). Retrieved from https://www.csis.org/analysis/recruiting-and-retaining-cybersecurity-ninjas

5. Reed, D., Yung-Hsu Liu, A., Kleinman, R., Maestri, A., Reed, D., Sattar, S., Zeigler, J. (2012, July 25). An Effectiveness Assessment and Cost-Benefit Analysis of Registered Apprenticeship in 10 States. Retrieved from https://wdr.doleta.gov/research/fulltext_documents/etaop_2012_10.pdf

6. Reinhold, M.D. (2016). Memo. [OPM; CHCO Council]. Retrieved from https://www.chcoc.gov/content/requirements-federal-cybersecurity-workforce-assessment-act

7. Requirements of the Federal Cybersecurity Workforce Assessment Act. (2016, August 01). Retrieved from https://www.chcoc.gov/content/requirements-federal-cybersecurity-workforce-assessment-act

8. Robbins, G. (2017, April 17). Tons of $80,000 entry-level jobs going ignored. The San Diego Union Tribune. Retrieved from http://www.sandiegouniontribune.com/news/cyber-life/sd-me-connected-highered-20170417-story.html

9. Robinson, H. (2017, June 19). Teens join the cyber profession. Retrieved from http://www.csbj.com/2017/06/16/teens-join-cyber-profession/

10. Saporta, L., Bluet, T., National Governors Association (2014). Federal Cybersecurity Programs: A Resource Guide. Retrieved from https://www.nga.org

11. Scorton, G. (2017, July 3). Four Things You Must Do to Retain Top Tech Talent. Information Week. Retrieved from http://www.informationweek.com/strategic-cio/team-building-and-staffing/four-things-you-must-do-to-retain-top-tech-talent/a/d-id/1329241

12. Securing Our Future: Closing the Cybersecurity Talent Gap October 2016 results from the Raytheon-NCSA survey of young adults in 12 countries about cybersecurity career interest and preparedness [PDF]. (2016). Sterling, VA: Raytheon Intelligence, Information and Services. Retrieved from http://www.raytheoncyber.com/rtnwcm/groups/corporate/documents/content/rtn_335212.pdf