TEAM 8.1:

B Venkata Mounish Reddy(VIT- VELLORE,20BSD0149)

Codavali Praveen Jahnavi(VIT-AP,20BCB7072)

Gantegampu Akshitha(VIT-AP, 20BCB7065)

Rayudu Gayatri(VIT-AP,20BCB7058)

TOPIC: Security Awareness Training

Security awareness training is an important component of an organization's cybersecurity strategy. It entails training personnel and users about potential security dangers, best practises, and appropriate behaviours to adopt in order to safeguard sensitive data and prevent security breaches.

Here are some of the most important features of security awareness training:

1. Threat Awareness: Training sessions are designed to increase awareness of various cybersecurity risks like as phishing emails, social engineering, malware, and ransomware, as well as the need of being diligent in recognising and reporting suspicious activity.

2. Password Security: Employees are trained on the importance of creating strong, unique passwords as well as the importance of frequently updating and not sharing passwords.

3. Phishing Awareness: Employees are taught to be careful of suspicious emails, attachments, or URLs that may lead to the compromise of sensitive information in order to recognise and avoid phishing attacks.

4. Data Protection: Emphasis is placed on the significance of securing sensitive data and adhering to data protection policies, such as secure file handling, encryption, and secure disposal of sensitive information.

5. Device Security: Best practises for safeguarding devices are highlighted, including setting password protection, encrypting data, and exercising caution while using public Wi-Fi networks.

6. Social Engineering Awareness: Employees are trained on the social engineering techniques used by attackers to trick them into disclosing personal information, emphasising the importance of verifying identities and being wary of unexpected demands.

7. Incident Reporting: Employees are encouraged to report any security incidents, suspicious actions, or potential breaches to the proper organisational channels as soon as possible.

8. Compliance and Regulations: Employees are educated on industry-specific compliance regulations such as GDPR (General Data Protection Regulation) and HIPAA (Health Insurance Portability and Accountability Act) to ensure they understand their responsibilities while managing sensitive data.

Security awareness training should be done on a regular basis and reinforced via interactive sessions, simulations, quizzes, and continuous communication channels. It contributes to the development of a security-conscious culture within the organisation and lowers the chance of successful cyber assaults caused by human error or negligence.

RECENT ATTACKS

1. Microsoft Azure SSRF Vulnerabilities

Microsoft Azure services were susceptible to server-side request forgery (SSRF) attacks on January 17, 2023, due to four vulnerabilities. Azure Functions, Azure Machine Learning, and Azure Digital Twins were among the services offered. Lidor Ben Shitrit, an Orca researcher, claims that if these SSRF vulnerabilities had gone unpatched, they might have had a substantial effect on Microsoft Azure Services. These vulnerabilities were closed before they could do much harm thanks to Microsoft's quick response.

2. Slack GitHub Account Hack

Slack, one of the most well-liked commercial communication applications, was hacked on December 29, 2022. CyberInt, an Israeli security company, was responsible for the incident.

The investigation showed that a small number of employee tokens were taken and used improperly to access a GitHub project that was hosted externally. On December 27, the threat actor had also downloaded private code repositories, although neither the main codebase for Slack nor any client data were contained in those downloads. Slack quickly nullified the stolen tokens and got to work looking into how it might have affected their clients. The threat actor did not gain access to any other parts of Slack's system or client information, it was discovered.

3. Data of 228 Million Deezer Users Stolen

The well-known music streaming service Deezer, which has millions of customers worldwide, revealed a serious data breach that may have impacted millions of Deezer members when a hacker offered information from more than 200 million users for sale on a hacking website. Deezer claims that the data breach occurred in 2019 and that the hackers were successful in acquiring a copy of user data from a third-party service provider, with whom they had not collaborated since 2020.Deezer asserted that it had taken all necessary steps to work with the third-party service provider and ensure that security measures were in place. These steps included obtaining ISO 27001 and SOC 2 certifications, contractual obligations to secure data, GDPR-compliant data protection agreements, and certificates of data destruction at the conclusion of the engagement.

4. Twitter Leaks Data on 200 Million Users

On December 4th, 2023, a data gathering sale including more than 200 million Twitter profiles began. A 59 GB RAR bundle containing the stolen material was made public. The scrapers utilising earlier data collections were able to compromise the vulnerable API. Awareness of targeted phishing scam campaigns is advised for Twitter users. A threat actor on a cyber forum offered a data collection with more than 200 million Twitter profiles for sale on December 4th, 2023, for eight credits, which were finally made accessible for free on November 27, 2022. A second data dossier allegedly containing details on 17 million people was apparently making its way around secretly in November. Threat actors have been selling and sharing enormous data collections of scraped Twitter user accounts since July 22, 2022, on a variety of online hacker forums and markets dedicated to criminality. These accounts featured both personal and work email addresses, usernames, screen names, follower counts, account creation dates, and other publicly available information.

5. Malware Targets 30+ WordPress Plugins

For malicious intents, the Linux Trojan Application takes advantage of out-of-date WordPress plugins and themes. The malicious application has two versions, the second of which is an enhanced version of the first. Even if the plugins are updated, it's possible that the attackers will continue to target WordPress site administrators' accounts. A Linux backdoor worm has been found that can exploit about 30 WordPress plugins in order to insert malicious JavaScript code and send users to fraudulent, phishing websites that the attackers have constructed. Such exploits are possible because outdated plugin and theme versions are present on the susceptible WordPress sites. As a result, the attackers are able to execute these assaults because as soon as a user accesses a WordPress website that has been hacked, they are immediately forwarded to a malicious website

6. Kubernetes Clusters Hacked

Vulnerable images and improperly configured PostgreSQL servers were used as two possible points of attack. The attack's motivation is money-making and cryptocurrency mining. Cluster security for Kubernetes is a laborious task that must be completed. The threat actors behind the Kinsing Crypto Jacking operation have been observed using unprotected and incorrectly configured PostgreSQL servers in order to get early access to Kubernetes systems. Golang, a high level programming language designed to develop cloud native applications, was used to write the malware known as Kinsing. It is put together using Go 1.13.6. Typically, Linux installations are the major targets of this malware for cryptocurrency mining. The objective changes to invading other PCs once the malware has been successfully deployed and is operating successfully on the victim's system. Two attack vectors were used, according to an analysis of the attack by Microsoft security researchers. Establishing and listing the PostgreSQL servers that had setup problems is the first attack path. The "trust authentication" setting, which enables PostgreSQL to assume that any connection made to the server is authorised to gain database access, is one of the most frequent configuration errors that were being abused from there. Additionally, any IP address that the attacker may be using can be utilised to access the server if a security flaw results in a wide range of IP addresses being assigned. The second attack strategy aims to take advantage of a vulnerability in container images.

7. Covid 19 Pandemic

The pandemic, the lockdown, and the ensuing adaptations made by businesses and communities across the globe have changed how cyber security is perceived. The impact of the pandemic on cyber security is deep and pervasive. Thanks to the *bring-your-own-device* trend, remote workplaces, and the exigency of third-party applications, attackers are exploring new attack surfaces and there is a frightening number of new vulnerabilities.

8. The Ukraine-Russia War

Russia's information offensive against Ukraine since 2014 culminated in February 2022 with Russia's invasion of Ukraine. Ukraine's cyber defences against Russian attacks have been strengthened over time. As a result, the practical impact of Russian strikes during and after the invasion was minimal. Nonetheless, the security professionals of the globe, as well as the hackers, learned a lot from these occurrences.

9. The Emergence of RaaS Gangs

A number of Ransomware as a Service gangs, ranging from Doppelpaymer and REvil to Vice Society and Nevada, have posed substantial risks to businesses, individuals, and governments all around the world. Some were politically motivated, such as the Conti gang, while others, such as Vice Society, virtually solely target schools and other educational institutions. The advent of RaaS has compelled government agencies to reconsider security.

10. Attack on Tallahassee Memorial

Tallahassee Memorial Hospital provides 772-beds and special care units in 21 counties around North Florida. The hospital's IT systems were damaged by a suspected ransomware attack, forcing it to shut down all online processes for more than a week. All elective surgical procedures have to be rescheduled. Many patients were relocated to other facilities.

11. Attack on VMare ESXi

VMware ESXi is a Hypervisor that allows virtual machines to run. The corporation released a fix for the vulnerable OpenSLP in 2021, however it appears that many servers were not patched. "The ransomware encrypts files with the.vmxf,.vmx,.vmdk,.vmsd, and.nvram extensions on compromised ESXi servers and creates a.args file for each encrypted document"

12. Bank Accounts Hacked in Nepal

The police have arrested eight criminal actors in Kathmandu, Nepal, for hacking into bank accounts. The attackers used WhatsApp to distribute the Android package kit (APK) for a bogus app called Nepali Keti. They then stole money by hacking into the bank accounts of anyone who downloaded the programme.

13. XSS vulnerabilities found in DMS providers

The attack had happened on February 7 2023. Its targets were OnlyOffice, OpenKM, LogicalDOC, Mayan. Four DMS providers were said to have an XSS vulnerability - CWE - 79. The firms provide both free and freemium services. Rapid7 uncovered the zero-day vulnerabilities during a routine inspection.

14. 71 million request-per-second HTTP DDoS attack thwarted by CloudFare

Cloudflare thwarted the greatest known DDoS attack on February 14, 2023, with 71 million requests per second. The attack targeted gaming platforms, cryptocurrency organisations, and hosting providers, among others, which utilise Cloudflare to secure their websites. The assault used HTTP/2 and included 30,000 IP addresses.

15. Dish Network faced a data breach

Dish Network, one of the largest television providers in the United States, confirmed that the earlier reported network disruption was caused by a cyber assault. The underlying causes of the intrusion have yet to be discovered. The attack resulted in data theft and a breakdown in internal communication. Some data was extracted and Dish’s share fell by 6.5%

16. US Marshals Service faces ransomware attack

The US Marshals Service is in charge of sensitive operations such as federal judge security, fugitive apprehension, and so on. Attackers hacked the standalone USMS system, exposing data connected to USMS investigations.

17. T-Mobile Data Breach

T-Mobile, a wireless telecommunications operator in the United States, disclosed on January 19, 2023, that a bad actor had acquired access to some customer data via a weak API. According to their declaration, the breach exposed sensitive data such as credit card information or social security numbers.

18. Attack on AirFrance and KLM

Two major airlines, AirFrance and KLM, confirmed unauthorised access to consumer data in a recent study. Some personally identifiable information about Flying Blue customers was revealed as a result of the assault. However, no Passport, financial, or social security information was compromised. Flying Blue is a customer loyalty programme operated by several airlines.

19. Windows ALPC Zero Day

According to Microsoft, "A malicious user who successfully exploited this vulnerability could gain SYSTEM privileges." Particularly, on January 10, 2023, Microsoft released 98 updates, including one for the ALPC zero-day vulnerability.

20. Attack on Mailchimp

Mailchimp discovered unauthorised access to several Mailchimp accounts on January 11, 2023. Social engineering was employed by attackers to gain employee credentials for a tool utilised by MailChimp's customer-facing workers. According to Mailchimp's announcement, the hack was restricted to 133 accounts. The impacted accounts were shut down on January 12th and later reactivated.

21. A third-party data breach affected Nissan North America

Nissan North America revealed a data breach that occurred in June 2022 on January 16, 2023. The bad actor targeted a third-party vendor who had limited access to client data for development purposes. Nissan started an inquiry in September 2022, which revealed that the hack took advantage of the vendor's poorly built database.

22. Attack on PayPal customers

Credential stuffing is a cyber-attack in which hackers use automated techniques to submit thousands of stolen user IDs and passwords into consumer input areas. Credential stuffing works because people have a habit of using the same credentials for several accounts. For two days, hackers had full names, dates of birth, social security numbers, postal addresses, and individual tax identification numbers of 34,942 PayPal members.

23. Attack on schools in Tucson, Arizona, and Nantucket

Tucson Unified School District is the largest school district in Southern Arizona. Since their data was encrypted by a ransomware attack on the last weekend of January, the schools were forced to switch to an offline method of education. The hackers have demanded a ransom and threatened to reveal stolen material if payment is not made.

24. Exposition of Yandex source code

Yandex is a significant Russian technology corporation. Recently, 44.7GB of code repositories were uploaded as a Torrent on a hacker forum. According to the poster, the files contain Yandex Git resources. The corporation has denied that it was hacked. It has blamed the theft on a former employee and stated that the leaked source code is no longer in use.

25. Killnet targets US hospitals with DDoS attacks

KillNet is a Russian hacktivist organisation that has actively targeted US healthcare facilities, including Stanford University. The US Department of Health and Human Services has issued a warning about the attacks. KillNet is well-known for assaulting countries who fought back against Russia's invasion of Ukraine. Additionally, in Kaspersky's most recent quarterly report, 57000 DDoS attacks were registered in three months. DDoS attacks increased by 79% in 2022.

26. Attack on ION Group

After launching a ransomware attack against ION Cleared Derivatives, a part of ION Markets, on January 31, the Russian RaaS gang LockBit added ION Group to their data leak site, threatening to reveal sensitive investor data. This had considerable impact on derivative trading in Europe, the United States, and the United Kingdom.