SIGNIFICANT CYBER SECURITY VULNERABILITIES

Name of the Student

Institution

Course

Instructor

Date,

SIGNIFICANT CYBER SECURITY VULNERABILITIES

ABSTRACT

Cyber security vulnerability signifies a defect in a host or information technology system that hackers might capitalize on against you.   
An information technology resource can be compromised and a hacking attempt can be furthered when vulnerability is exploited. Organizations must find and fix vulnerabilities in order to improve their overall cyber security posture. Among many potential cyber security flaws include outdated hardware, misconfigured cloud services, unpatched software, as well as poor authentication software.

**SIGNIFICANT CYBER SECURITY VULNERABILITIES**

Cyber security vulnerability is a flaw that can be exploited by cyber criminals to compromise an organization's internal controls, information systems, or operations of the system. The aforementioned weaknesses do offer points of entry for intruders to enter a computer system without authorization, which may jeopardize private information or result in damage. Among them are the following’

Weaknesses found in the source code. Potential vulnerabilities in the code occur during the software development process. Logical mistakes may result in security issues, such as the creation of an access privilege lifecycle that an attacker may exploit. If the software employs randomized encryption strings, they could fail to be sufficiently random or it might unintentionally transport substantial information without encryption. If the software development lifecycle is too long, many developers may work on a project, which could lead to the incompleteness of some functionality. All of these vulnerabilities need to be identified and addressed during testing, but they might affect businesses by affecting the supply chain as a whole (Perkins, et al., 2009 October).

System elements that are incorrectly setup. Another typical mistake made when setting up enterprise IT systems is misconfiguration. At the most basic level, for example, an administrator can neglect to modify the software's default settings, which would leave the system exposed.. Cloud systems that are improperly designed, misconfigured networks, hastily assembled Wi-Fi setups, (Adegoke, et al., 2013). practices and threats related to cloud computing's service availability. And even failing to impose restrictions on the use of non-work devices could significantly increase your exposure to risk. Thankfully, fixing these vulnerabilities is not too difficult. They usually arise from an overworked IT staff that needs assistance from a managed organization.

Arrangements pertaining to trust. Trust arrangements are the compromises you make for data communication between hardware and software systems. For example, a mounted external device may be able to read confidential data from an operating system client without a user's consent. Active directories and account records might include trust connections, which could allow unrestricted data flow between sources that aren't continuously monitored. Sheth (2014) was A. N. These trust arrangement flaws give an attacker the ability to take control of a compromised system, spread the virus from that compromised system, and eventually destroy your whole IT infrastructure.

Weak procedures for credentialing. One of the most frequent reasons for vulnerabilities in commercial and consumer systems has been identified as this. Users frequently adhere to convenient or comfortable credentialing procedures, putting usability ahead of security. For instance, using a browser's built-in password manager to store passwords and account credentials has become standard practice, despite advice from experts to the contrary. Vulnerabilities include weak passwords that reuse personal information such as your name and those that employ common alphanumeric characters (123456, password, etc.). There are two ways to reduce these security flaws: by raising user knowledge and enforcing credentialing procedures like password expiration.

Insufficiently secure encryption. Unencrypted data transfer poses a serious risk and may result in serious security breaches. Data encryption makes sure that someone with malicious intent cannot decode or understand the information in the event that Goyal, V., & Kant, C. (2018) lose control of your primary storage platform. Regretfully, encryption is still not keeping up with the rate of digital transition and the resulting document digitization. While mobile data storage is currently the main focus of encryption, research Opens a new window indicates that enterprises have not yet addressed this issue in USB sticks, laptops, and portable hard drives. Both while data is in transit and at rest, it should ideally be securely encrypted.

Internal danger. Finding and fixing insider threat vulnerabilities is difficult, particularly when it comes to remote work. According to Forrester, insider threats will account for 1 in 3 security breaches in 2021—an increase of 8% over the previous year. There are several reasons why your employees could be at risk from insider threats, including insufficient hiring practices and background checks, internal conflict inside the organization, and external geopolitical events. Given that most employees work from home, it might be difficult to spot unusual activities that might indicate an internal threat within your organization.

psychological vulnerability. Psychological vulnerabilities are also caused by people, just like insider threats are, but they happen accidentally and affect everyone. Human conduct is driven by basic psychological drives such as the need to defend oneself, the desire for exceptional benefits, and the fear of danger. Typically, social engineering is used by hackers to exploit these flaws. They convince users that in order to gain an advantage or avoid a negative situation, they need to act in a certain way. A simple example is a psychological bug that leads many people to click on emails that seem to be offering promotional discounts, thereby infecting their machines with malware.

Inadequate authentication. Authentication vulnerabilities arise from insufficient checks and balances that need the reset of credentials and passwords. This suggests that a hacker might access your account through the "forgot password" function present in all login systems, search for a backdoor, and then initiate an account takeover (ATO) attack. One example of a too-easy-to-guess authentication question could be your birthdate, which is publicly available on social media. Alternatively, multi-factor authentication, which guards against account security being compromised by a single hacked device, might not be used by the system.

Exposed sensitive information. Exposed sensitive data might happen in a number of ways. Data can accidentally be published to a database that is frequently thought of or posted to a public website. A single employee could become the owner of a sizable database containing highly sensitive data simply because of improper access controls. These situations don't necessarily include malevolent intent, in contrast to data breaches. Sensitive data, which could include intellectual property, user credentials, personally identifiable information, payment details, etc., could possibly end up in the incorrect location and be exploited due to human error or system misconfiguration.

Segmenting and monitoring the network insufficiently. Many attackers rely on inadequate network segmentation and monitoring after they have gained initial access in order to take total control of every computer inside a network subnet. Networks of large companies have historically been vulnerable to this severe cyber security vulnerability. Attackers are now far more tenacious when it comes to accessing new systems and staying there for a long time.   
inadequate tracking and recordkeeping. Regular log analysis and comprehensive log recording are essential for reducing security risks. M. Souppaya and K. A. Kent (2006). If not, it's possible for someone not permitted to access your computer environment and nobody will know about it until it's too late. Unexpected system signals typically point to the existence of a hacker or malicious bot and can be found via log analysis.

Vulnerabilities related to share tenants are an unavoidable aspect of the cloud era. Public cloud solutions use a multi-tenant architecture, where different organizations lease out a shared set of resources at different periods based on how much resource each organization needs.

Nonetheless, the management may choose to use the following to resolve the issues mentioned above:

Invest in endpoint detection and response solutions with reaction capabilities, behavioral analysis, and next-generation antivirus software. These tools offer more versatile options for prevention and detection as well as a more thorough analysis of malicious conduct. Forensic details and compromise signs, real-time response capabilities, and enhanced behavioral inspection are features that users of traditional antivirus software should think about upgrading to.

Implement a multifaceted recovery and backup procedure. This should cover end-user storage, which is frequently cloud-based, database storage, tape or disk backups, and snapshots and replication of data center storage. Seek out enterprise-class solutions that support comprehensive monitoring and reporting for backup and recovery.

Pay close attention to regulating network access between subnet systems and developing more effective detection and alerting mechanisms to prevent lateral movement between systems that shouldn't be in communication with one another. Keep an eye out for strange DNS lookups, strange behavioral patterns in network traffic, and system-to-system communication that doesn't seem to be useful. More restricted restrictions for traffic and system communications can be established with the aid of proxies, firewalls, and micro segmentation tools.

Establish strict password policies. This could include using longer, more complicated passwords and rotating them more frequently. Generally speaking, long and strong passwords that aren't changed frequently are more secure than shorter ones that are. Additionally, password-less authentication helps stop users from selecting bad passwords. Require multifactor authentication for every sensitive access, frequently with the use of MFA solutions, before allowing users to access sensitive data or websites.

Organize frequent training sessions that address social engineering, pretexting, and phishing. Numerous training courses are offered to support the reinforcement of security awareness principles. Whenever possible, users should be trained on relevant and contextualized to the work tasks personnel. Utilize "live fire" tests with phishing emails and other techniques, and monitor the success or failure rates of users' testing. If a user's performance remains unchanged, consider remediation strategies that are suitable for your company.

REFERENCES

Perkins, J. H., Kim, S., Larsen, S., Amarasinghe, S., Bachrach, J., Carbin, M., ... & Rinard, M. (2009, October). Automatically patching errors in deployed software. In *Proceedings of the ACM SIGOPS 22nd symposium on Operating systems principles* (pp. 87-102).

Adegoke, A., & Osimosu, E. (2013). Service Availability in Cloud Computing: Threats and Best Practices.

Enck, W., Gilbert, P., Han, S., Tendulkar, V., Chun, B. G., Cox, L. P., ... & Sheth, A. N. (2014). Taintdroid: an information-flow tracking system for realtime privacy monitoring on smartphones. *ACM Transactions on Computer Systems (TOCS)*, *32*(2), 1-29.

Goyal, V., & Kant, C. (2018). An effective hybrid encryption algorithm for ensuring cloud data security. In *Big Data Analytics: Proceedings of CSI 2015* (pp. 195-210). Springer Singapore.

Kent, K. A., & Souppaya, M. (2006). Guide to Computer Security Log Management:.