Vulnerability Management Policy

IT Knowledge Hub LLC (dba "Knowledge Hub Media")

Author

IT Security Officer

Authority

Knowledge Hub Media - Chief Executive Officer (CEO)
IT Knowledge Hub LLC - Chief Executive Officer (CEO)

Purpose

The purpose of this policy is to define the requirements for notification, testing, and installation of security-related patches on devices connected to Knowledge Hub Media networks.

Vulnerability Management & Cybersecurity Policy

It is the stated goal of the Knowledge Hub Media and IT Knowledge Hub LLC to provide secure IT resources and services in order to protect institutional information assets, as well as the privacy of individual clients, customers, vendors, officers, employees, staff members, independent contractors and other entities with which the institution has contractual obligations.

In doing so, Knowledge Hub Media and IT Knowledge Hub LLC must comply with applicable laws, regulations, and other corporate or unit policies regarding protection of systems and data. The timely and consistent application of vendor-supplied security patches or mitigation of a reported vulnerability are critical components in protecting Knowledge Hub Media and IT Knowledge Hub LLC network, systems, and data from damage or loss due to threats such as malware, viruses, data breaches, data loss, denial-of-service (DoS), distributed denial-of-service (DDoS), man-in-the-middle (MitM), phishing, spear phishing, SQL injection, and/or other types of external or internal attacks.

Knowledge Hub Media and IT Knowledge Hub LLC authorized the IT Security Office and Information Security Office to conduct routine scans of devices connected to Knowledge Hub Media and IT Knowledge Hub LLC networks to identify operating system and application vulnerabilities on those devices.

Knowledge Hub Media and IT Knowledge Hub LLC require all administrators of systems connected to Knowledge Hub Media networks to routinely review the results of vulnerability scans and evaluate, test and mitigate operating system and application vulnerabilities appropriately, as detailed in the Vulnerability Management Process. Should an administrator identify a reported vulnerability as a potential false positive, the appropriate security office should be engaged to verify.

Scope

This policy applies to all departments and schools of Knowledge Hub Media and IT Knowledge Hub LLC. This policy applies to all electronic devices connected to Knowledge Hub Media or IT Knowledge Hub LLC networks (public and private) including but not limited to computer workstations and servers, network switches and routers, cloud servers and platforms, and specialized hardware equipment, etc.

Responsibilities

System and application administrators are responsible for assessment and application of security patches that impact systems under their management and supervision.

Exceptions

Requests for exceptions to this policy (requests to not scan a device) may be granted for systems with other security measures (e.g., network filtering, firewall, etc.) in place to mitigate risk.

Any requests must be submitted in writing to the IT Security Officer and/or Chief Executive Officer for review and approval. Exception requests must include:

- Why the scanning exception is being requested.
- Risk to the enterprise of not scanning the device.
- Mitigation controls that have been implemented, and date of implementation.
- End date for the exception (not to exceed 6 months from the request date).
- In the case of systems or applications managed by internal IT staff, endorsement of the request by the relevant IT staff.

Enforcement

It is the responsibility of system and application owners to ensure that the policy described in this document is followed. IT administrators understand that the secure implementation of systems and applications is a critical part of Knowledge Hub Media's overall information security strategy.

The Knowledge Hub Media IT Security Office and the IT Knowledge Hub LLC Information Security Office are authorized to limit and/or block access to vendor, client, customer, employee, staff member, independent contractor and corporate officer network or datacentre access, for any and all devices, applications, and security practices that do not comply with this policy.

Definitions

Data Breaches - A data breach is a security incident in which information is accessed without authorization. Data breaches can hurt businesses and consumers in a variety of ways. They are a costly expense that can damage lives and reputations and take time to repair.

Data Loss - An error condition in information systems in which information is destroyed by failures or neglect in storage, transmission, or processing. Information systems implement backup and disaster recovery equipment and processes to prevent data loss or restore lost data.

Denial-of-Service Attack (DoS) Attack - A DoS attack overwhelms a system's resources so that it cannot respond to service requests.

Distributed Denial-of-Service (DDoS) Attack - A DDoS attack is also an attack on system's resources, but it is launched from a large number of other host machines that are infected by malicious software controlled by the attacker.

Malware Attack - Malicious software can be described as unwanted software that is installed in your system without your consent. It can attach itself to legitimate code and propagate; it can lurk in useful applications or replicate itself across the Internet. Some of the most common types of malware are macro viruses, file infectors, system or boot-record infectors, polymorphic viruses, stealth viruses, trojans, and ransomware, among others.

Man-in-the-Middle (MitM) Attack - MitM attacks occur when hackers insert themselves between the communications of a client and a server. Some common types of man-in-the-middle attacks include, but are not limited to, session hijacking, IP spoofing, and replay attacks.

Phishing Attack - The practice of sending emails that appear to be from trusted sources with the goal of gaining personal information or influencing users to do something. It combines social engineering and technical trickery. It could involve an attachment to an email that loads malware onto your computer. It could also be a link to an illegitimate website that can trick you into downloading malware or handing over your personal information.

Spear Phishing Attack - A more targeted type of phishing attack. Attackers take the time to conduct research into targets and create messages that are personal and relevant. Because of this, spear phishing can be very hard to identify and even harder to defend against. One of the simplest ways that a hacker can conduct a spear phishing attack is email spoofing, which is when the information in the "From" section of the email is falsified, making it appear as if it is coming from someone you know, such as your management or your partner company.

SQL Injection Attack - SQL injection attacks tend to be common issues with database-driven websites. It occurs when a malefactor executes a SQL query to the database via the input data from the client to server. SQL commands are inserted into data-plane input (for example, instead of the login or password) in order to run predefined SQL commands. A successful SQL injection exploit can read sensitive data from the database, modify (insert, update or delete) database data, execute administration operations (such as shutdown) on the database, recover the content of a given file, and, in some cases, issue commands to the operating system.

Virus Software - A type of malicious code or program written to alter the way a computer operates and is designed to spread from one computer to another. A virus operates by inserting or attaching itself to a legitimate program or document that supports macros in order to execute its code. In the process, a virus has the potential to cause unexpected or damaging effects, such as harming the system software by corrupting or destroying data.