THE SafeHarbor™ BRIEF

Gnostech Inc. Maritime Cybersecurity Newsletter - July 2018

COMBATTING COMMON CYBER THREATS

Best Practices - PART 1

As part of the User Education and Awareness series, previous newsletters discussed the importance of user education and provided greater awareness regarding phishing and malware. This issue will build on topics previously discussed and provide general best practices for all users. The practices listed below will establish a general knowledge of basic cybersecurity concepts to add another layer of security for any enterprise network.

User Education and Training

> **Human error accounts for 52% of the root cause of security breaches.**
> *- CompTIA*

As the theme of this newsletter series suggests, one of the most important practices for good cyber hygiene is education and developing a comprehensive user training program. Users should be required complete an organizational training program before gaining access to your enterprise network. Users should also be required to take an annual refresher course. Training programs should be updated regularly as external events occur or changes are made within your company's enterprise network.

Data Backups

Backing up your company data is essential to minimize loss and maintain operational "uptime" during any incident, whether it be a natural disaster or cyberattack. Best practice dictates that that companies should complete a full backup of their data once a week, with a differential incremental or cumulative incremental backup for every day that a full backup is not completed. Full backups typically occur when it is least disruptive to a company's operations, such as on the weekend or late at night. Tape backups should be encrypted and stored at an off-site location when possible. If that is not possible, due to cost, tapes should be encrypted and stored locally in a fire proof safe. Personnel with access to tape backups should be approved by management through proper documentation and should be limited in terms of what they can access.

Password Complexity

Global Policy Objects (GPOs) should be complexity and strength rules. Password strength is determined by the amount of characters required for a password; the minimum recommended is about 14

PROTECT THE ENTERPRISE NETWORK BY MAKING PASSWORDS MORE COMPLEX.

Ensure that your company's passwords are secure by increasing password length, having a variety of uppercase and lowercase letters, special characters, and numbers.

characters. Password complexity is what makes up the password characters; a decently complex password should consist of upper and lower case alphabetical characters, special characters (%, $, &, etc.), and numbers. Password policies should also restrict the use of common dictionary words and the reuse of the same password a set number of times in a row (i.e., users cannot use a password they have already used in the last 180 days). It is highly recommended that users are required to change their passwords every 90 calendar days.

Note: Encourage your users to never write down their passwords. Physical copies of passwords result in physical security risks that can be easily stolen and used to gain access to your company's enterprise network.

Separation of Duties

The separation of duties is the concept of having more than one person to complete a task, especially for sensitive or critical assets. For instance, it is not considered best practice for a company to only have one administrator with access to all boundary defense assets. If that person leaves the company under bad terms, they could bring the entire network enterprise down. What if they suffer from an unforeseen accident and can no longer relinquish their control over the enterprise network? These examples may seem extreme, but it is always something to consider and remind ourselves why the separation of duties is so imperative.

Firewalls

Firewalls are typically your first line of logical defense for your enterprise network. Firewalls are used to filter incoming and outgoing traffic through a network of access controls lists (ACLs); depending on the type of firewall deployed, this network security system can also offer many other types of services. These services can include spam filters, packet inspection, Intrusion Detection System (IDS), and Intrusion Prevention System (IPS), just to name a few.

Types of firewalls to consider:

- Packet-filtering Firewall
- Circuit-Level Gateway
- Stateful Inspection Firewall
- Application-level Gateway
- Next-gen Firewall (combines network traffic filtering with another functionality such as an IPS)

Establish Clear and Concise Policies and Procedures

Policies are essential to a company's business as it helps employees to clearly identify company expectations based on job positions, company business strategies, and objectives. Procedures identify how to perform day-to-day operations and steps to take in the event of an incident. Policies and procedures should be updated regularly to match any changes to company expectations; management should always approve and sign off on company policies and procedures. In addition to updating policies, a process for employees to review and receive training on current policies will help with ensuring policies and procedures are followed.

Multi-Factor Authentication

Multi-factor authentication is a security concept that requires more than one method of authentication to grant network access to computer systems or physical access to rooms and buildings. Authentication can be broken down into different types of factors, to establish a multi-factor authentication company would require at least two of these factors to gain access to system or buildings. These factors include the following:

Something you know – a password or personal identification number (PIN)

Something you have – a smart card or token (RSA SecurID token)

Something you are – biometrics identification (fingerprints, retina scan, etc.)

Somewhere you are – physical location through Global Positioning System (GPS)

Something you do – known pattern on a touch screen or graphoanalysis

Patch Management

Patch management is the process of updating your computer system software to fix vulnerabilities identified in the software by either software developers or a successful attack (whether malicious or non-malicious). Companies should have a patch management process established to patch their systems regularly in order to prevent possible risk to their enterprise network.

For most malicious actors, well known vulnerabilities in common system software will be the first area they try to exploit. Unknown vulnerabilities or exploits by software developers or the cybersecurity community are referred to as a zero-day vulnerability. Unfortunately, these types of vulnerability are most often discovered by malicious attackers first and used immediately before they can be discovered and patched by the software vendor. These types of vulnerabilities should be patched as soon as a patch is available and tested.

About Gnostech Inc.

Gnostech Inc. is an applied engineering and consulting company with over 35 years of experience and expertise in information assurance and cybersecurity engineering, and major combat and space systems development and integration. Gnostech provides the necessary knowledge and technology to ensure success of critical missions for customers in both the defense and maritime industries. To learn more, visit www.gnostech.com.