THE SafeHarbor™ BRIEF

Gnostech Inc. Maritime Cybersecurity Newsletter - September 2018

ESTABLISHING COMPANY GUIDELINES AND POLICIES

Plans and Policies - PART 1

Company plans and policies can help establish organizational guidelines, personnel expectations, and protect against legal action in some cases. Our goal for this month's newsletter is to help our maritime industry partners create structured plans and policies to manage their company's overall cybersecurity posture. *Gnostech develops comprehensive plans and policies that follow the National Institute of Standards and Technology (NIST) Cybersecurity Framework.* This newsletter will provide a high-level overview of the various documents an organization should consider developing and their purpose. Please note that not all company policies require a detailed back-up plan to support it.

Account Management

Account management is a type of access control that maintains the creation, modification, and decommissioning of user accounts. There are many components a company should consider when developing an account management policy:

- Companies should identify the personnel responsible for account creation, usually security administrators
- A formal request for an account that requires a physical signed copy by the requesting user (which should then be filed away and kept for auditing purposes
- Company authentication and password complexity standards
- Separate account requirements, to include the initial request, user roles and privileged user accounts

Configuration Management

NIST Special Publication (SP) 800-128 defines configuration management as "a collection of activities focused on establishing and maintaining the integrity of products and systems, through control of the processes for initializing, changing, and monitoring the configurations of those products and systems."

In simple terms, this means establishing a policy to define major changes to a company's computer systems and/or infrastructures. It is recommended that a Configuration Control Board (CCB) be established within your company to convene and discuss any proposed changes to the enterprise network. A proposed change can be submitted by anyone within the company, but will typically come from your cybersecurity team or security administrator(s). An example of a significant change includes upgrading from Windows 7 operating system on all user computer systems to Windows 10. It may not seem like a significant change to some, but upgrading one's operating system could break the functionality of applications he or she uses for their day-to-day tasks. Careful planning, consideration, and testing should be done by the CCB before implementing major changes to the enterprise networks. Changes agreed to by the CCB should be documented thoroughly for auditing purposes and for maintaining your current enterprise network baseline.

Disaster Recovery

In this case, a Disaster Recovery Plan or Policy (DRP) are synonymous. This document is crucial to preventing a total loss of data in the event of a major incident, cyber or natural, and bringing critically identified systems back online as soon as possible. Essential for any company, a DRP is a very large document comprised of many plans. Having a comprehensive DRP in place can save company revenue. It is that important! Here are a few important components that should be placed within

How Much Does 1 Hour of Downtime Cost the Average Business?

Major IT outages cause losses of $100,000 per hour in medium-to-large enterprises, according to an Information Technology Intelligence Consulting study. Having an effective DRP in place is critical to reduce recovery time and mitigate business impact.

a DRP to determine what must be done to limit the damage and protect systems from a cyberattack:

Emergency Response Plan - Who is contacted when a major disaster occurs? When are they contacted in the process (escalation)? What immediate actions must be taken upon discovery of a disaster? This plan should also identify alternates in case personnel are unavailable.

Business Impact Assessment (BIA) - While not necessarily a plan, a BIA should be conducted to determine a quantifiable value for critical network enterprise assets. Believe it or not, all assets within your enterprise, including personnel, have a monetary value attached to them and how they affect your business. For instance, if Amazon had a single database that housed their product listings and it went down one day, they would lose millions in revenue. A BIA should be conducted along with a risk assessment to determine which critical assets are at a higher risk and need additional measures to protect them.

Back-up and Restoration Plan - This plan identifies the frequency of back-ups for your enterprise network and should identify which systems take priority in the recovery process of a disaster (which are identified as part of the BIA). This plan should also identify responsible personnel, procedures for safe keeping of back-ups, and regularly testing back-ups to ensure they are working as intended.

Media Strategy - Identify personnel to engage with the media in the event of a major incident and determine what they can disclose to the public. Depending on the size of your company, you may seek legal or retain legal counsel to handle all communication with the media.

Vulnerability Management

Vulnerability management is a security practice designed to proactively prevent the exploitation of vulnerabilities within an application's firmware or software (mostly through patching). The vulnerability management policy should identify:

1. Responsible personnel who would apply patches

2. How patches are prioritized (assigning a value of criticality)

Patch testing and deployment in a development environment should be required before applying them to your company's production environment. The vulnerability management plan should list the detailed process for each item within the policy. Most vulnerability management is managed through automated security tools; the step-by-step procedures should be documented in the plan, as well as how to report metrics (for auditing purposes).

Cybersecurity Training and Awareness

Although we have covered this topic a few times in previous newsletters, there should be a formal policy and plan in place for user education. A formal policy is necessary to determine frequency of training requirements, requiring personnel to compete company developed or adopted training programs before being given access to the enterprise network, and an acceptable use policy. The plan should detail how the items detailed in the policy should be accomplished by your training personnel. There are many considerations to be made when developing a training plan, such as how often to test your users on current cyber threats, how training records should be maintained and protected (for auditing purposes), and how a training plan should be focused depending on job roles and functions within the company.

Companies should also consider adopting an acceptable use policy that defines expectations of user activity on company owned assets. This policy should specifically define what is not considered acceptable use, as well as potential ramifications for deviating from the policy, such as termination.

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.