THE SafeHarbor® BRIEF
Gnostech Inc. Maritime Cybersecurity Newsletter - November 2018

ESTABLISHING COMPANY GUIDELINES AND POLICIES

Implementing an Acceptable Use Policy

In previous newsletters, we discussed standard policies an organization should implement to ultimately improve security posture. This month, we will focus on one policy in particular. In today's interconnected world, it is vital to have an acceptable use policy. This policy is an integral part of any organization's security measures, and can help protect against cyberattacks.

What is Acceptable Use?

Acceptable use policies restrict the ways in which an organization's networks, websites, or systems may be used, and set guidelines as to how such resources should be used. It is not unusual for users to sign this type of policy before being granted access to enterprise resources.

Most acceptable use policies limit or outright ban resource use for personal gain, such as:

- running a personal company
- web site hosting
- soliciting
- spamming
- downloading unapproved software or content

Such inappropriate use can expose organizations to virus attacks, compromise of network systems and services, and legal issues.

It should be of significant priority to have an acceptable use policy in place, to be both used and enforced. Without an acceptable use policy in place that employees acknowledge and sign off on, an organization will have a very hard time enforcing any corrective action against an individual who may have shown poor judgment.

Some general items to consider when developing an acceptable use policy are highlighted below. The depth and breadth of an organization's acceptable use policy may be guided by existing requirements of the organization, industry, country, or customers through a Memorandum of Understanding or Agreement (MOU or MOA).

Purpose

Determine and define what the organization is trying to convey and accomplish when generating an acceptable use policy. Ensure that the proposed acceptable use policy is compatible with the current industry and government standards. Develop a policy that is implementable and enforceable. An acceptable use policy should not be viewed as punitive, but as a common understanding of what is expected when interfacing with and handling organizational data.

Acceptable use policies are vital to protect the security of an organization's network and prevent users from introducing viruses or opening their systems and the entire network to attacks.

Instructions and policies are key with BYOD.

The majority of businesses embrace some form of BYOD, but 77% of employees say they did not receive instruction in the risks of using their own devices at work and only 64% of companies have a BYOD policy in place.

Policy Scope

Determine what is and is not included in your acceptable use policy. Your organization should assign a Point of Contact (POC) to lead and administer the acceptable use policy. In addition, reviewing the acceptable use policy on a regular basis with your stakeholders is necessary to stay current with any technological changes. Most organizations, regardless of their area of influence, have a need for an acceptable use policy.

The Positive and Negative Impacts

An organization must evaluate the benefits and drawbacks of an acceptable use policy before it is embedded within an existing organization. With the introduction of an acceptable use policy, your organization may need to manage how the employees react to the policy. Organizations should illustrate the need and value of an acceptable use policy, as well as emphasize the consequences of not having a policy in place.

Understand Your Data and Determine What is Important

Determine what level of importance your data is to the organization. Over time, changes to the operational environment can change visibility and data priority. Organizations should review the prioritization of data and access. Contracts, pricing, personally identifiable information (PII) and proposal information should be viewed with high importance and reviewed for restricted access to most employees.

Government Rules and Regulations That May Affect Your Acceptable Use Policy

Regulations continue to change and affect how organizations must comply. Your organization must make sure that its acceptable use policy does not affect their compliance with government regulations. Specific examples include PII, Health Insurance Portability and Accountability Act (HIPAA), and Sarbanes–Oxley Act (SOX). State, Federal, and International laws are not always compatible, so a determination will need to be made as to what regulations an organization must follow. If your organization deals with European companies or organizations, the new General Data Protection Regulation (GDPR) requirement may impact your organization. If data is to be made available for use between countries, ITAR (foreign export requirements) may need to be reviewed and implemented. The government has information and agencies to provide guidance to your organization.

Bring Your Own Device (BYOD)

On top of acceptable use in an organization is the growing popularity of BYOD for both work and use. Many organizations find BYOD policies to be highly beneficial; employees are adept at using their own technology, so organizations can cut its technology, software, and refresh budget.

A BYOD policy may seem all but negative, but it is important to consider its implications. An organization must consider who – either the organization or the employee – will pay for virus or malware remediation on a personal device. An organization must also decide if they should be responsible to push virus and patch updates to an individual's device. In addition, it is important to consider if the organization has a right to scan or confiscate a personal device for any reason.

Social Media

Does your organization currently have a social media process or POC? A majority of organizations embrace social media for promotional purposes, but allowing employees access to social networking sites can open them up to malicious content, phishing schemes, and account hijackings. Organizations do not own these sites and thus have no influence in enforcing strong passwords and vulnerability management. Consider identifying acceptable use parameters that accommodate both personal and business engagement.

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.