THE SafeHarbor™ BRIEF

Gnostech Inc. Maritime Cybersecurity Newsletter - April 2018

COMBATTING COMMON USER THREATS

User Education and Awareness

What is cybersecurity?

Cybersecurity is defined as measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack. The purpose of this newsletter is to define basic level cyber threats for any organization. This topic will span the next few newsletters posted by Gnostech. Users and their system access or permissions within a network enterprise are often targeted first by bad actors in order to circumvent an organization's cybersecurity policies and mechanisms. User education is the first step in minimizing risk to your network enterprise. A user, in this case, is any person(s) operating a computer system owned by a company and used to handle official company business. Frequent user training and testing will increase their awareness on current cyber threats and trends and help to create an effective, multi-layered security architecture (defense-in-depth) for your network enterprise. In order to be successful, a cultural change throughout the company, from executive level to the hands-on personnel performing the work, is needed to build the initial security chain of prevention.

Important user education and training program concepts

Identify what data your organization handles that is considered sensitive or classified. There are many factors that can determine what sensitive data means to your organization, including contractual obligations and government/country defined sensitive data. Users should be made aware of what is considered sensitive or classified data and what the consequences could be for mishandling or misrepresenting such data. Identifying this type of data should not used as a scare tactic, but to educate users on the impact it may have on the organization to have this data stolen. Government or company sanctions should be provided within an Acceptable Use Policy that users are required to sign before given access to a company network enterprise. Sanctions should be clear and concise so users understand the severity of mishandling sensitive data.

Supervisory Control and Data Acquisition (SCADA) system protection should be heavily emphasized to any user/operator that will have access to or work with on a daily basis. The devices that comprise a SCADA system will be considered highly sensitive for any company that employs them. Users with access to these systems should have additional training and be required to sign policies and agreements specific to the SCADA system.

Promote a safe reporting environment for users. The previous section mentions identifying sanctions for the mishandling and misrepresentation of sensitive and classified data and educating users on such consequences. Users should understand the penalties a company could face legally. Ensure your training program is written in such a way that a user feels empowered to report an incident to a security team without fear of strict personal ramifications. The primary objective for a company is knowing what is going on within the network enterprise at all times, and knowing is half the battle. Users should feel safe to report any type of incident, such as phishing attempts, social engineering, or a proprietary data spill. Employ the concept of "if you see something, say something". Encourage users to report anything they may consider to be suspicious even if it ends up being a false positive. This allows your security team to evaluate all potential threats and potentially prevent them before it causes severe damage to the enterprise network.

Address Insider threats

An insider threat is a malicious threat to an organization the comes from people within the organization; however, insider threats can be either accidental or malicious. An accidental insider threat

USER EDUCATION IS YOUR FIRST LINE OF DEFENSE.

Train personnel regularly to ensure they understand core cybersecurity concepts and know how to identify a potential threat to your enterprise network.

can occur if a user falls victim to a phishing scam, plugs in a USB device into a system that contains a virus (without their knowledge), or discloses sensitive company data or proprietary data to someone outside the company. In these cases, the user inadvertently creates a security risk due to a lack of user education and did not intentionally mean to harm the company or enterprise network. A malicious user, on the other hand, engages in these types of activity knowingly. A malicious insider threat is deliberately trying to sabotage a company's assets for monetary gain or a personal vendetta. Common ways to help prevent insider threats include implementation of a least privilege, separation of duties, user education, and logging of user activities. Least privilege is the practice of only giving a user the network permissions needed to perform their job. Separation of duties is the concept of having more than one person required to complete a task to prevent fraud and errors.

Manage and Mitigate User Risk

Produce a security policy that incorporates acceptable use policies and identifies user roles and responsibilities. The security policy should also list job roles and the expectation for each position within the company. Also ensure that users are given only the appropriate permission to perform their job. An acceptable use policy should detail what the company deems appropriate for user activity on their enterprise network. Ensure all new users review and sign an acceptable use policy that can be filed away securely in the event of an incident or audit.

Train users at least quarterly to ensure they are aware of the company policies and any current cyber threats. Require new hires to complete all company training before being granted access to the network enterprise. Maintain records or all user training through signed letters and certificates. Again these signed forms should be securely filed in the event of an incident or audit.

Test users periodically and find deficiencies in your user training program. Security teams should create fake phishing emails or perform mock social engineering tactics to identify where their training and security deficiencies are. This will allow the security team to create a more robust security training program and help close gaps in their user risk.

Produce a disciplinary process (formal). Users should be inclined to freely report incidents as they happen on the network, but there should be disciplinary actions for purposefully negligent actions that could harm the network. Users are going to make mistakes from time to time and that is okay. What you are looking to prevent in this situation is habitual offenders. If a user is constantly trying to download from malicious Internet links or trying to plug in personal mobile devices, you may have an insider threat and there should be associated consequences. Company leadership should find a balance between having their users freely report accidental incidents while still adhering to their own policies to maintain company asset integrity and provide protection against any legal ramifications that could arise based on the sensitivity of an incident.

Gnostech can provide a comprehensive user training program tailored to address specific maritime threats if necessary.

Available Resource

NIST Special Publication 800-50, Building an Information Technology Security Awareness and Training Program:

https://csrc.nist.gov/publications/detail/sp/800-50/final

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.