IT'S CYBERSECURITY AWARENESS MONTH!

Updates from the Office of Internal Controls, Audit Compliance & Information Security (IAC/S)

Welcome to the final weekly segment for Cybersecurity Awareness Month. This week we're focusing on the new MDH security posture and expectations of our personnel.

THERE IS NO FINISH LINE.

One of the key topics we are highlighting is the importance of everyone's continued focus on cybersecurity. Just because you won't be hearing from the Security Team weekly doesn't mean that we can rest on the knowledge that we are safe. Unfortunately, in today's environment cyber criminals continue to create and implement new Attack Vectors and take advantage of Zero Day Vulnerabilities. Emerging threats remain something we monitor and address daily.

Recent Examples to Learn From

Two recent examples of major breaches showed us that even with security tools in place cyber criminals have successfully brought down some major targets.

Case 1: The entire Costa Rican government was brought to its knees due to a ransomware attack that lasted for weeks: Ransomware gang threatens to overthrow Costa Rica government | AP News

Case 2: In a recent L.A. Public Schools case, hackers launched a ransomware attack over Labor Day weekend, in line with the strategy of "back to school" and holiday attacks that target stressful times: Los Angeles schools ransomware attack: Cybercriminals release hacked data, superintendent says | CNN

What MDH has done to secure our environment

2022 was a busy year for MDH in implementing tools and procedures to protect us from cyber attacks. The MDH Info Security 3-year strategic plan was greatly accelerated, and a new plan is in development based on the new Cyber Security posture.

Listed below are some highlights:

- **Network Management:** allows remote workers to have frictionless, highly secure access to the enterprise network from any device, at any time, in any location while protecting the organization
- **EDR (Endpoint Detection & Response):** solutions that are very effective in collecting continuous information on malware footprints and other types of potential cyber threats to the network
- **Active Directory & Network Management:** allows you to perform various tasks such as managing printers, install software via 'snapins' and change host names and joining Active Directory (for Windows machines)

- **Golden Image:** a cloned disk that can be used as a template for various kinds of hardware to provide a consistent and predictable format for disk images. Golden images ensure all necessary software and security measures are installed on a drive from the very beginning, allowing IT managers to create the consistent environments where the end user doesn't have to know a lot about the technology for it to be used effectively.
- **Managed Next Generation Firewall (NGFW) Services:** combine many of the capabilities of traditional firewalls --including packet filtering, network address translation (NAT) and port address translation (PAT), URL blocking, and virtual private networks (VPNs)--with quality of service (QoS) functionality and other features not found in traditional firewalls. These include intrusion prevention, SSL and SSH inspection, deep-packet inspection, and reputation-based malware detection, as well as application awareness.
- **Security Incident and Management (SIEM):** makes it easier for enterprises to manage security by filtering massive amounts of security data and prioritizing the security alerts the software generates. SIEM software enables organizations to detect incidents that may otherwise go undetected.
- **Enterprise Endpoint Protection:** software that protects these points of entry from risky activity and/or malicious attack. When companies can ensure endpoint compliance with data security standards, they can maintain greater control over the growing number and type of access points to the network.
- **Vulnerability Management:** a program designed to keep your network safe from known exploitations and ensure it stays compliant with any regulatory requirements. It does this by analyzing your network fo any incompatibilities, missed updates, and common weaknesses within the software you use.
- **Email Encryption:** designed to prevent all kinds of inadvertent release of sensitive data, whether it's because an unauthorized user gains access to the email communications channel or if an internal user accidentally emails it to the wrong recipient.

In conclusion, 2022 has been an amazing year for us as far as implementing various tools and processes to secure our environment.

Please visit the MDH Information Security intranet page: https://mdho365.sharepoint.com/sites/InformationSecurity/

To access this page use the same instructions (attached to this email) for accessing the overall MDH Intranet pages. The Intranet site does not require users to be connected to the MDH network (no VPN needed).

- Your username is your **MDH Active Directory username** (i.e., the same username you use to log into your computer) followed by **@maryland.gov**
- Your password is your **MDH Active Directory password** (i.e., the same password you use to log into your computer)

Thank you for your continued attention as it relates to supporting this extremely important initiative. Remember: there is no finish line.