An Attractive Target: Why Cyber Hygiene Matters

Does Digital Hygiene Matter?

Threat actors often look for the easy target, scanning the internet for unpatched vulnerabilities, and probing your defenses for the weakest part of the chain. Poor information technology digital hygiene, such as expired secure sockets layer (SSL) certificates or faulty URLs, can draw attention to your company to these threat actors during their explorations. During the reconnaissance phase of the Cyber Kill Chain, the attackers are assessing what is easiest for them to exploit and their findings during exploration could mark your company as an attractive target for them to pursue.

Effective cyber hygiene is a challenge for the entire organization and not just the IT department responsible for your network. IT hygiene revolves around the maintenance of data integrity and availability. Cyber hygiene focuses on security processes such as rotation/strong password rules, scheduled virus scans to keep environment from any potential malware infection. Ensuring that both types of hygiene are up to date can make a difference in how your company is perceived by threat actors, as well as the added benefit of reducing your reputation risk from researchers citing bad online practices by your business.

Avoiding the Targeting Poor Hygiene Gets You

Every business that maintains an online presence or connectivity needs to keep up to date with the ever-evolving cyber threat landscape. It is not possible for your cybersecurity team to mitigate all the threats your organization might be facing without the active support and awareness of the rest of the company. It is the responsibility of your entire organization to practice hygiene best practices.

Key Best Practices

Maintain an updated inventory list of all your equipment and software

This is one of the most important lists an organization can complete. A proper inventory list is required to complete a proper network architecture map. By having a complete network map, it will be much easier to implement security policy, configure appliances, and prioritize what assets are of critical to operation.

Hardware: Any end user devices, connected devices such as printers, servers, and mobile devices that will be used on the organization's network.

Software: All software that are installed directly onto organization's devices.

Applications: Software as a Service (SAS), applications on mobiles devices, and any other program that isn't directly installed on devices.

Ideally, your inventory list will also be updated with current change management and configuration management processes. Beyond knowing what product you use, you should also be able to understand the latest version deployed and how it is configured for your environment.

Analyze your company assets and programs

When a complete inventory list has been completed, it will be easier to analyze the list for potential vulnerabilities for mitigation and remediation. The list should be used to make sure all software and apps are kept updated and passwords should be changed. For example, unused equipment should be taken off the network and properly disposed

of, and an updated list should be able to show whether this has been actioned upon or not. Prioritizing assets in terms of criticality for business operations to continue and costs of replacing them, contributes to your risk management of these systems as well.

Along with technical assets, a company should consider their skilled personnel capable of managing these assets and the hygiene that goes with them. Smaller firms may outsource some of their hygiene duties, and other businesses may need personnel to wear multiple hats in terms of responsibilities. When possible, leverage a "right skillset to the right role to the right outcome" mindset when defining roles and responsibilities.

Keep a common hygiene policy throughout your firm

A firm will need a common set of practices to maintain proper cyber hygiene no matter if they have outsourced some or all of these activities. These practices should be documented into a set policy to be followed by all who have access to the network. For larger enterprises, the policy should ensure an open dialogue between the Chief Information Officer's offices and Chief Information Security Officer's teams.

- Keep software updated: Updating the software that is used by the organization should be part of a hygienic review. Remove legacy systems (and data), especially when no longer supported by manufacturer security updates.
- Do not hold onto hardware for too long: Older end user devices may need to be updated to prevent issues and maintain performance.
- Keep up with your asset/inventory list: Every new installation(s) of devices and software should be documented to keep an updated inventory list. Ensure monitoring to establish baseline behaviors to ease discovery of anomalous activity.
- Limit user access: Only those who require admin level access to devices and software should have access. Other users should have limited capabilities to prevent any unauthorized access. Need to Know and Zero Trust practices should be followed when possible.
- Change your passwords: Complex passwords policy and change cycle can prevent various malicious activities.
- Back up what you need to become operational again: All data from the organization's devices and apps should be backed up to a secondary source segmented away from the primary network. This will ensure the backup's safety in the event of breach and will also allow for response remediation to cyber attacks such as ransomware.

Once a cyber hygiene policy is created, each task should be scheduled at a specific timeframe. For example, password changes should be every month, and running a vulnerability scan at specific intervals. Implementing a comprehensive cyber hygiene best practice will assist maintaining a sound security posture for organizations.

Developing comprehensive cyber hygiene procedures is a must for today's enterprises. When carried out in conjunction with robust enterprise-wide security practices, sound cyber hygiene practices aid in maintaining a sound security posture for modern organizations.