secpod

Why Cyber Hygiene?

BEST PRACTICES FOR ORCHESTRATING CYBER HYGIENE

WHITEPAPER • APRIL 2020

“Good hygiene leads to sound well-being”

As this saying goes, right now everyone in the world is practising sound hygiene methods to prevent themselves from the viral COVID 19 pandemic. Since the widespread of the pandemic is increasing day by day, the Government has imposed strict laws and is educating the people to practice good hygiene methods.

Personal hygiene is extremely pivotal today. But, how about cyber hygiene?

The way we all take care of ourselves, it is necessary to take care of the system health and IT security as well. We never know when an attack might intrude into an organization network and invade the IT security. It is always better to stay preventive than be a victim of security breaches.

90% of breaches involve known vulnerabilities for which a patch were available but not applied

75% of organizations infected with ransomware were running up-to-date endpoint protection

The total cost of a successful cyber attack is over $5 million, or $301 per endpoint

Why is Cyber Hygiene crucial for an organization?

Organizations are expanding across the globe and the safety of their IT network is of primary importance to them. There are numerous ways through which organizations' IT security can be exploited.

Attackers are working in full force to figure out the security loopholes in the network and are waiting to cause severe security havocs. A lot of big players in the market can be named who have badly suffered the misery of cyber attacks and have put their brand reputation at stake.

A study says at the end of 2016, a business fell victim to a ransomware every 40 seconds and this is expected to rise to 11 seconds in the year 2021. Most of the cyber attacks could have been easily prevented if regular cyber hygiene measures were in place. But the pitfall for many businesses is they don't practice proper security measures to safeguard their IT network.

About 50% of organizations haven't updated their security strategy for more than 3 years. All this emphasizes the need for the organizations to follow effective cyber hygiene practices to prevent their network from various security breaches.

10 Best Practices to Orchestrate Cyber Hygiene

1 Run continuous asset scan and get complete visibility of your hardware and software inventory.

The number of hardware and software used by an organization keeps increasing day by day. Enterprises need to get complete visibility of these devices and monitor them thoroughly. IT administrators should run a regular scan on the enterprise systems and get details of all the hardware and software available in the network.

This not only helps organizations make planned purchase moves, but it also helps them identify the entry of any malicious or unwanted assets into the network environment. To orchestrate cyber hygiene, the foremost practice organizations should follow is to keep a close eye on the hardware and software assets.

2 Analyze software usage metrics, blacklist malicious assets and manage license violations.

Once the details of the hardware and software assets are available, it is important to track the usage metrics. This allows organizations to get data on the software which are being highly used and eliminate the usage of any software which poses a threat to enterprise IT security and employee productivity.

After detecting such malicious software, IT administrator should blacklist them immediately to prevent further usage. Along with this, it is also necessary to track the software license details and detect the systems which violate the license regulations.

3 Evaluate system health, check the details of user login, services and processes regularly.

When it comes to personal health, getting regular health check-ups done is an advisable practice. Similarly, in an IT network assessing the system health regularly is a crucial step. Enterprises should continuously monitor the system health of the endpoints and track the user details.

IT teams should thoroughly monitor vital details like user logon time and place, details of services and processes running in the system, system registry details etc., to validate if any hazardous security activities are happening in the network.

4 Ensure antivirus software is available in each system and is updated on time.

One of the most important cyber hygiene practices is to check if each system in the network contains an anti-virus software. Anti-virus software acts as a security gatekeeper in each system which protects them from viruses and alerts them on any potential threats.

Also, it is not sufficient only if the anti-virus software is available, it is crucial to check if this software is regularly updated on time. Remember that having un-updated antivirus software is equivalent to having no software at all.

5 Perform vulnerability scanning every day and assess the detected vulnerabilities.

Vulnerabilities can enter the systems in many ways. These vulnerabilities can lead to various malware and ransomware, putting IT security in danger. It is pivotal for the IT team to run a regular vulnerability scan in the network and fetch details on the available vulnerabilities. It is recommended to perform this vulnerability scan daily to tighten the IT security.

After fetching the vulnerability details, IT administrators should access and analyze the vulnerabilities thoroughly to predict potential threats. It is highly advisable to prioritize Vulnerabilities based on its severity range to plan further remediation measures.

6 Patch OSs, un-updated software and critical vulnerabilities without any delay.

Patching is one of the most crucial cyber hygiene measures recommended to safeguard IT security. Many of the major ransomware attacks like WannaCry could have been easily prevented if patching was done on time. Patching not alone helps organizations provide their employees with the latest updated version of the software, it also saves them from a variety of vulnerabilities.

Companies run across multiple software installed on various OS platforms. It is pivotal to get this software and OSs patched then and there. Also, patching is considered a critical technique to remediate vulnerabilities. After detecting and assessing the vulnerabilities, it is important to remediate them through patching technique.

7 Instantly block applications, USBs and other peripheral devices posing security threats.

Various exploits, security breaches and data threats can set foot into the network through the usage of malicious applications, USBs and other peripheral devices. Many organizations have experienced data breaches because of staying lethargic to the entry of these applications and devices.

To secure organizations sensitive information, it is recommended to block these devices and applications instantly. IT Teams should continuously monitor the network, detect the entry of these malicious applications and devices and block them without any delay.

8 Identify deviated system settings and enforce compliance and security benchmarks.

According to various important compliance benchmarks like HIPAA, PCI, ISO, NIST etc., the computers in the network should contain various system settings and configurations. Deviations in any of these system settings might lead to various security breaches.

Administrators should constantly monitor the network and identify the systems which are not abiding these security standards and enforce compliance benchmarks on them immediately. If required, IT Teams should create its own security policy and enforce them on enterprise computers. This is often considered a crucial step in securing the devices.

9 Impose strict password policies and prevent users from setting weak system passwords.

Having a weak system password automatically paves way for the attackers to break into the IT network. Simple short length passwords like abcd@123 are easily guessable and will allow hackers to try brute force attacks.

To safeguards enterprise security, it is a mandatory measure to impose strict password policies like including characters, capital letters, numbers and determining the length of the password. Although this looks like a very simple measure, it is a very important and a basic step to secure the enterprise endpoints.

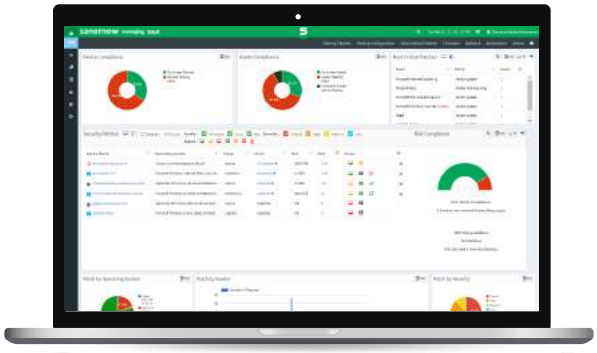
10 Detect any indications of attack and system compromise and respond to them immediately.

In many organizations, there will be a lot of computers having abnormal system settings which might be the indications of attacks. Some computers might have been already comprised of cyberattacks and will be still prevalent in the network environment.

It is vital to identify the computers showing these indications of attacks and compromise and respond to them immediately. IT Teams should identify such computers in the network and act upon them to secure their enterprise from any potential breach.

SECPOD **SANERNOW**

Revolutionary platform to orchestrate and automate cyber hygiene



In this book, we saw how crucial it is to implement cyber hygiene in the network and the best practices to orchestrate them. However, getting all these cyber hygiene measures orchestrated is not a simple task. Also, it is important to note that these practices are not just a one-time task and are needed to be followed in the IT network continuously.

A platform which will not only orchestrate but also automate this entire task of cyber hygiene will be of great help to IT administrators. SecPod SanerNow is the one solution which will get all these done in a few simple steps. All you must do is deploy Saner agents on your target computers and the rest is automatically taken care by the SanerNow server, through which all actions can be performed and managed.

Start Free Trial
of SanerNow

What you can achieve with SanerNow?

Asset Management

Continuously perform regular asset scan on the enterprise endpoints and get clear visibility on all the hardware and software available in your network. You can effectively assess and manage the enterprise assets to ensure effective usage for the business and safeguard IT network from the entry of malicious assets.

Vulnerability Management

Regularly scan, detect, assess, prioritize and remediate vulnerabilities without any hassles. This allows organizations to automatically identify the critical vulnerabilities, assess their risks and exploitation potential, prioritize them based on the severity and mitigating them instantly.

Patch Management

Automate patch management on Windows, MAC, LINUX OSs and a variety of third-party applications like Adobe, Google, Java, Mozilla etc., and secure your enterprise endpoints from critical vulnerabilities. This patching technique can be completely automated and scheduled to recur daily.

Compliance Management

Identify the computers not abiding by security standards and enforce compliance on them immediately. Stay compliant by meeting various compliance requirements and security standard benchmarks like PCI, HIPAA, NIST 800-53 and NIST 800-171. You can choose to create own security policies and map them with enterprise endpoints.

Endpoint Management

Get complete control of your enterprise endpoints and manage them easily from a centralized console. You can install or uninstall any software, perform registry and various system setting, apply changes to existing services and processes, block any malicious applications, USB and other peripheral devices etc.,

Threat Prevention & Response

Continuously monitor, detect and respond to advanced threats. Identify the indications of attack and compromise in the network and act upon them immediately. Eliminate the gap between threat detection and response and provide an adherent threat protection to the endpoints in your network.

About SecPod, Inc.

SecPod is leading provider of endpoint security and management solutions. SecPod (Security Podium, incarnated as SecPod) has created revolutionary SanerNow platform and tools that are used by MSPs and enterprises worldwide. SecPod also licenses security technology to top security vendors through its SCAP Content Professional Feed.

To learn more about SecPod, visit: www.SecPod.com

SecPod, Inc.

303 Twin Dolphin Drive, 6th Floor,
Redwood City, California 94065, USA.

Contact

Sales : info@secpod.com
Support: support@secpod.com
Phone: (+1) 918 625 3023 (US)

secpod