25 Best Practices for Basic Cybersecurity

Prioritize These Steps for a Successful Cybersecurity Plan

- ❑ **Remove local administrator access for all users** – Local admin access by users is a high risk if user credentials get compromised.

- ❑ **Limit user's access to only the data/systems needed for their role** – Make sure there are no shares or privileges for user's accounts to data that they do not need. "Least privilege access" decreases the ability of an attacker to gain access to all data by compromising a single user's credentials.

- ❑ **Do not allow anonymous access to anything** – Scan your network to enumerate all shares. Add permissions to any with anonymous access and remove any default logons from devices (i.e. admin/admin).

- ❑ **Use secondary accounts for all admin access** – When admins use these accounts for daily use the admin accounts are exposed to increased risk of credential theft. Keep the usage at a minimum.

- ❑ **Use long, non-string passwords for all admin and service accounts** – Administrator accounts and service accounts are primary targets of threat actors. Make them difficult with a password management tool to maintain the complex passwords.

- ❑ **Terminate sessions after a period of inactivity –** Session stealing is a common practice. Don't expose these sessions any longer than necessary.

- ❑ **Only allow remote access through encrypted channels** – Use Multi-Factor Authentication (MFA). Remote access is a huge threat vector and requires additional technical controls.

- ❑ **Do not expose RDP to the internet** – RDP weaknesses and vulnerabilities are well known and easy to exploit.

CNP TECHNOLOGIES

FORESITE
VISIONARY SECURITY & COMPLIANCE SERVICES

- ❑ **Use some form of wired network access controls** – Basic MAC address filtering adds an extra layer of security by checking the device address against an approved list.

- ❑ **Separate the Guest wireless from Production** – Guests should never be allowed on the production network.

- ❑ **Use WPA-2 enterprise with authentication for production wireless access** – A passphrase is not enough as the wireless usually extends beyond the walls.

- ❑ **Stop using USB storage except where absolutely required** – USB storage is a method used to infect with malware and increases risk of data leaks.

- ❑ **Ensure all systems stay patched** – All applications and devices such as firewalls; not just Windows patches.

- ❑ **Use a modern antivirus** – Next-gen AV can respond to behavioral threats, not just a database of known virus signatures.

- ❑ **Review everything that you are allowing through the firewall on the internet** – Networks can allow things on the internet via the firewall that open them up to threats. Make sure you know what is allowed and why, and make sure the firewall is patched regularly.

- ❑ **Provide security awareness training for all users** – Users often can be a weak point. Make sure they understand the risks, the latest threat tactics, and what to do if they receive a suspicious request.

- ❑ **Preserve critical logs** – Logs should be shipped off critical servers and devices and preserved in case they are needed for incident investigation.

- ❑ **Implement spam filtering** – Email is a major threat vector. Spam filters can flag and block suspicious messages.

- ❑ **Implement physical security for critical systems** – All critical and sensitive servers and network equipment should have limited physical access. Visitors should always be escorted.

- ❑ **Password hygiene** – Train users not to save passwords in clear-text files. Use at least 12-character complex passwords and force scheduled changes.

- ❑ **Multi-Factor Authentication** – Use MFA for any access coming from the internet, including VPN, webmail, and cloud services.

- ❑ **Destroy any data device before disposing** – Shred hard drives, destroy removable media, and render the data unrecoverable.

- ❑ **Remove user access to anything and everything after terminations** – A process should be in place to remove access when people leave the organization, including 3rd party vendors that have system access.

- ❑ **Plan for worst case scenarios** – Make sure you know what to do if there is an incident such as ransomware or business email compromise. **Have resources in place** before you need them to speed up response.

- ❑ **Scan for vulnerabilities** – Scan all internal and external devices on your network as often as possible to detect and remediate known vulnerabilities.

Contact us for more information:

CNP Technologies

www.cnp.net

(888) 973-3737

info@cnp.net

CNP TECHNOLOGIES

FORESITE

VISIONARY SECURITY & COMPLIANCE SERVICES