EAGLE NETWORK SOLUTIONS™
80 Palomino Lane Suite 202 • Bedford, New Hampshire 03110
A Division of Enchanted Ventures, LLC

Basic Network Security Recommendations

Server & PC Security Privileges

• No domain admin rights for users. This is the superuser account, the "keys to the kingdom." If exploited, it carries the highest rights on the network controlling all PC's and all servers.

• Set a lockout policy for failed logon attempts.

• No local administrator access.

Pro: Not having this right means that some malicious software is not able to run by accident. Most users are not *trying* to run malicious software.

Con: A user cannot install software including updates, printers or software. They have to call help desk.

Remote Access

• Best if not remoting into PC's, but only for file access. If desktop access to a PC is necessary, then only by a two-factor process of a VPN + Remote Desktop. Directly accessing a PC or server from offsite using Remote Desktop Protocol (RDP) should not be done. Using the latter requires a port to be open on the internet side of your firewall which is more frequently being hit by hackers to attempt unauthorized access. Recommend turning off RDP port redirects on the firewall to any internal PC's.

Pro: Significantly reduces outside attempts to log onto an internal PC by hackers.

Con: It requires a second step to establish a secure connection, and in most cases, firewall licensing.

Updates & Patching

• PC's and servers should be patched and updated regularly. This is acheived through user intervention where they are able to say yes to updating when prompted, but not if they are not a local admin. When given the chance to update, most do not because it takes time. This can be done in several ways, including a managed service offering that does this automatically. Bi-Monthly updates are recommended.

• Firmware is a type of patching for hardware such as switches and firewalls. This is an occasional manual process. Service agreements with the respective vendors are usually required. Quarterly checks are recommended.

• Up to date antivirus is critical for anything with an OS.

Network Security

• Audit user list regularly.

• Password should be min. 7 characters, require complexity, be changed frequently and not repeat past passwords.

• Folder security should be done by security groups when possible. Practice "security by obscurity" by hiding sensitive folders from users that should not see them. Restrict read/write access to only folders that a user absolutely needs to change. If they only need to view it, then don't allow them to change it.

• No phones on the corporate WIFI.

Pro: Folder security keeps your data safer from deletion or malice (virus, etc.) Password changes defy patterns that can be exploited.

Con: Tighter security is difficult to get used to.

Always have a backup