Matrixforce®

IT Provider Remote Transitioning

As an IT provider, we know that your clients rely on your assistance when transitioning to a remote, work from home environment. Whether that transition is short-term or permanent, remote working poses many new risks for the security of your client's data. Concerns that arise in a remote work environment include employee-owned devices (laptops, PCs, etc.) entering your client's network and spreading viruses or malware, employees not knowing how to use a VPN to access the network, employees letting their guard down when in comes to verifying the legitimacy of emails, and the list goes on. As their trusted security advisor, we strongly recommend assisting your clients in the development of remote work from home policies and procedures that will enforce strong guidelines to help protect their organization.

We've developed a list of guidelines and tips to assist you in ensuring your clients and their employees are prepared to work from home in a safe, functional work environment. Note, this list is intended for guidance and information purposes only.

Guidelines & Tips

- Ensure your client's firewall is capable of VPN traffic and ensure they have enough VPN licenses
- Test your client's Unified Communication strategy and technology: VOIP phones, softphone technology that transfers to mobile phones from your client's office number and your client's use of internal chat technology like Teams and Slack and video conferencing
- Enable encryption on your client's local devices (laptops and PCs)
- Local devices (laptops and PCs) should not have admin privileges. If they do, ensure strong passwords are required
- Limit your client's external sharing through Cloud applications (OneDrive, etc.)
- Enable a Mobile Device Management software on all your client's devices
- Ensure that any Bring Your Own Device (BYOD) personal devices meet your client's policy standards and include proper security and remote wipe capabilities
- Review and enable your client's remote endpoint security tools to ensure that they can be centrally reviewed and monitored for your client's company and employee-owned devices
- Provide your client with the ability to securely exchange files and information externally and internally (i.e., office-365 encryption option enabled, on-premises solution, etc.)
- Limit the access to Sensitive Company Information, Personally Identifiable Information (PII), and electronic Protected Health Information (ePHI) when your client's employee is not using a secure workspace or device
- Enable Multifactor Authentication for remote connectivity
- Ensure your client's remote connectivity sessions are set to expire after 4-8 hours
- Review Incident Response procedures with all relevant parties
- Educate your clients and their employees on common social engineering and phishing scams, including new scams relating to current events