corsica
technologies

CYBERSECURITY CHECKLIST

Recommendations to Accomodate Remote Workers

As more and more organizations encourage their employees to work from home, their cyberattack surfaces are increasing commensurately. Even if your organization has a strong cybersecurity posture, employees connecting from unpatched and/or compromised home computers dramatically increases the likelihood of credential theft, unauthorized access, data loss, and propagation of malware.

Below are some high-level recommendations that will help to protect against these cyberthreats.

□ Restrict Network Access

Wherever possible, restrict network (VPN) access to only company-issued and -managed computers. These are more likely to be up to date on patches and protected by anti-malware software. Configuring your organization's VPN server to require certificate-based authentication is a great way to ensure that only these computers are permitted to connect. Note that this would first require your organization to distribute certificates to eligible computers via an enterprise Public Key Infrastructure (PKI) or similar method.

□ Patch Management

Ensure that remote computers' operating systems and applications are fully patched. New vulnerabilities are discovered and announced every day, and each one represents a potential chink in your organization's armor. Fortunately, modern operating systems and most applications support the automatic download and installation of patches, but users should still verify that their systems are up to date.

□ Update Operating Systems

Ensure that all remote computers are running a currently supported operating system. The use of outdated operating systems like Windows XP, Windows 7, and Windows 10 dramatically weakens an organization's ability to defend against cyberattacks. Patches and hotfixes are no longer developed or supplied for these operating systems, and as security researchers and hackers continue to discover new vulnerabilities, unpatched systems could negate the other protective controls that an organization has deployed. You're only as secure as your weakest link, and outdated operating systems create an awfully weak link.

□ Install Anti-Malware

Similarly, ensure that all remote computers are running some type of anti-malware software (commercial package or built into the operating system) and that signatures are up to date.

□ Use a DNS Security Service

Use a DNS security service such as OpenDNS Home to prevent your users' computers from being able to resolve and connect to malicious domains. Approximately 95% of known ransomware strains require the ability to resolve malicious names in order to take hold, so this control is a highly effective countermeasure in the fight against ransomware. It's straightforward to implement and doesn't require advanced technical knowledge.

□ Implement Multifactor Authentication (MFA)

Implement multifactor authentication (MFA) and use it everywhere it's supported, but particularly in conjunction with publicly accessible services such as Office 365, SharePoint Online, remote-access VPN, and the organization's DNS administration portal. Any computer in the Internet-connected world could conceivably attempt to log into these services, and traditional passwords do not provide a sufficient level of protection. Many users reuse their Active Directory account passwords for their personal accounts on other websites, and if an attacker were to breach a site and obtain those credentials, he or she could use them to obtain access to the organization's systems or mailboxes. In addition, a user could easily fall prey to a phishing attack and disclose his or her credentials in response. In certain situations, MFA can be defeated by a resourceful attacker, but it's still much better than using passwords alone to prevent unauthorized access. Many vendors offer tried-and-true MFA solutions, and more and more systems support MFA integration every day.

□ Register Remote Employees with a Mobile Device Management (MDM) Platform and/or MAM Platform

If your organization uses a Mobile Device Management (MDM) platform or Mobile Application Management (MAM), ensure that remote employees' computers and mobile devices have been registered with it. An MDM platform extends organizational control to remote and mobile devices that have access to company data. It allows an organization to control security parameters and permitted apps, compartmentalize and control company data, and wipe devices that are lost or stolen. In the case of employee-owned devices, MAM is a better choice. It offers control over company applications and data without exercising excessive control over an employee-owned device.

This infographic highlights a number of technical measures with which your organization can more securely accommodate remote workers, but there's always more that can be done. Cybersecurity is a never-ending process of continuous improvement, not a destination at which your organization can suddenly arrive. There's no magic cybersecurity bullet, so defense in depth is the only viable strategy for surviving in today's threat landscape, particularly when so many employees are working from home.

As more and more organizations encourage their employees to work from home, their cyberattack surfaces are increasing commensurately. Even if your organization has a strong cybersecurity posture, employees connecting from unpatched and/or compromised home computers dramatically increases the likelihood of credential theft, unauthorized access, data loss, and propagation of malware.

Below are some high-level recommendations that will help to protect against these cyberthreats.

- □ Restrict Network Access
- □ Patch Management
- □ Update Operating Systems
- □ Install Anti-Malware
- □ Use a DNS Security Service
- □ Implement Multifactor Authentication (MFA)
- □ Register Remote Employees with a Mobile Device Management (MDM) Platform