Outdated Cybersecurity Practices That Are Putting You At Risk

Recent years have seen incidents of cyberattacks grow exponentially, with cyber threats often evolving faster than many organizations can keep up. Unfortunately, this can leave businesses vulnerable, as they may not know what they need to do to keep their digital assets secure. Even worse, for organizations that are unaware of these new cybersecurity threats, legacy security habits can provide a false sense of protection while leaving critical gaps, making them increasingly vulnerable to cyberattacks. To help ensure that your business has the best chances of defending itself against malicious actors, keep reading as we take a look at outdated cybersecurity practices that are still surprisingly common, and better alternatives that you should be using.

Overreliance on Traditional Antivirus Solutions

While cyberthreats have become increasingly complex, there's still a common misconception that traditional, signature-based antivirus solutions alone provide sufficient protection. However, this antivirus software often fails to provide robust protection against modern cyber threats, such as zero-day exploits and fileless malware. Yet, many organizations believe that as long as they have antivirus software installed, this guarantees that their data is protected. The reality is that achieving an effective cybersecurity posture now requires a layered approach that includes implementing Endpoint Detection and Response (EDR) solutions that offer real-time threat detection by monitoring endpoint activities.

Using Only Passwords (Without MFA)

While requiring your team to use robust passwords is essential in order to protect your network from threats, using only passwords is no longer enough, as passwords still remain a weak link in cybersecurity. This means that if you're relying on passwords alone to verify user identities, you're leaving your network vulnerable. Instead, you must enforce multi-factor authentication (MFA) across all accounts and services. Enforcing the use of MFA within your organization can go a long way in helping keep your data secure, especially when combined with least-privilege access controls.

Believing Firewalls Alone Will Protect You

Many businesses gain a false sense of security from their firewall, as they believe that a firewall is all they need to protect their network. However, perimeter-based defenses are outdated in a cloud-based, remote work environment. The fact is that firewalls don't account for lateral movement within networks, and relying on your firewall alone to protect you could leave you vulnerable. Instead, it's essential that you adopt Zero Trust architecture and micro-segmentation. Adopting a never trust, always verify mindset by implementing continuous authentication and least-privilege access protocols provides more effective defenses than a firewall alone.

Relying on Manual Software Updates and Patch Management

One of the biggest mistakes you can make is relying on manual software updates and patch management. The fact is that outdated software is one of the biggest causes of cyberattacks, as outdated software often contains vulnerabilities that hackers can exploit. However, if you rely on a manual patch management strategy, you may forget to perform timely updates, which could leave your network vulnerable. This makes it essential that you implement an automated patch management system to ensure timely updates.

Blind Trust in VPNs for Remote Access

In a modern, hybrid work environment, it's also essential that you do not blindly trust VPNs to provide sufficient protection for remote access. The fact is that VPNs don't always receive updates to defend against the latest cybersecurity threats, which could put your business at risk. Instead, you should use secure access service edge (SASE), ZTNA, or identity-based access controls. These methods provide more secure access for remote workers and offer a proactive method for safeguarding data.

Security Awareness Training Once a Year (or Less)

As you are likely already aware, your team is your first line of defense against cyberattacks. This makes security awareness training essential, as it updates your staff on the latest cybersecurity threats and steps that they should be taking to protect company data. Yet, if you're performing security awareness training once a year (or less), you could be putting your data at risk, as

cyberthreats are constantly evolving. The fact is that security training needs to be continuous, interactive, and scenario-based to ensure that your team is prepared for the latest cyber threats.

Failing to Conduct Regular Risk Assessments

A critical step many companies fail to take when boosting their cyber defenses is conducting regular risk assessments. The fact is that regularly conducting risk assessments that include vulnerability scanning and penetration testing is essential to ensure that you have a strong cybersecurity posture. A risk assessment evaluates your existing infrastructure for potential vulnerabilities that a hacker could use to access your data. A thorough risk assessment is then critical, as it will show you where your infrastructure is vulnerable and provide solutions that you can implement to better secure your company's data. Risk assessments should be carried out regularly and can be performed internally if you have a comprehensive IT department; however, small organizations with limited resources may find it beneficial to contract an outside vendor to perform a risk assessment for them.

Unmonitored Admin Access and Broad Privileges

An outdated practice many organizations still employ is giving users permanent, excessive admin access "just in case." However, attackers can exploit privileged accounts quickly and quietly. This is why it's essential that you use the principle of least privilege, as access should be limited to the data employees need specifically for their jobs. Using practices like Just-in-Time access, role-based access controls, and privilege auditing can limit who has access to sensitive data, reducing the risk of cyberattacks.

Storing Critical Backups in the Same Environment

While performing regular backups is essential in order to protect your business in the event of a cyberattack, these backups could be vulnerable if they are stored in the same environment as the rest of your data. If your backups are connected to your network, then ransomware can reach them as well. In order to ensure that your backup data is properly protected, it should be stored on a separate network or cloud environment from the rest of your data. A modern backup system should also be encrypted and include redundancy, such as secondary offline backups stored off-site.

If you've been relying on any of these outdated cybersecurity practices, the fact is that you could be putting your business in a dangerous situation. If you continue to maintain the status quo rather than adapting your cybersecurity practices to the latest threats, you may soon find yourself facing a costly data breach. This makes it essential that you regularly review and update your security posture to stay resilient against modern threats.

If you need help adapting your cybersecurity practices to meet evolving threats, consider giving [redacted] a call today.