Devolutions

5 Quick Wins for SMB Cybersecurity in 2021

THIS ARTICLE WAS WRITTEN BY THE PETRI TEAM IN PARTNERSHIP WITH DEVOLUTIONS.

There is no doubt that security incidents are on the rise for businesses of all shapes and sizes. With the recent pandemic, it has been clear that cybersecurity threats have become a bigger issue than ever before.

However, there is a common belief among many small and mid-sized businesses (SMBs) that the most lucrative vulnerabilities only exist in large organizations. But the fact is that SMBs are more vulnerable to cyberattacks than larger businesses and there are several reasons for this.

First, although larger organizations tend to have a bigger attack surface, these larger businesses also typically have specialized security personnel that are dedicated to protecting the organization. The skills and resources that they have available typically far exceed the capacities of most SMBs.

Second, the impact that cybersecurity or ransomware attacks can have on an SMB can be devastating. A larger organization typically has the resources to weather these types of attacks and although there may be significant downtime costs, the company typically will remain operational. That is not always the case for the SMB, as a lengthy service outage could have the potential to put them out of business.

In its State of Cybersecurity in SMBs in 2020 report, Devolutions surveyed SMB decision-makers worldwide and they uncovered several critical security exposures. First, 80% of SMBs admitted that malware has evaded their anti-virus software. Second, 66% of SMBs reported that they have experienced at least one cyberattack within the last 12 months and that each cyberattack typically resulted in an average of eight hours of downtime. Finally, and even more disturbing, 60% of SMBs have gone out of business within six months of a cyberattack.

Five Core Steps for Strengthening the SMB's Cybersecurity Protection

In the following sections, you will learn five core security strategies that the SMB can implement that will produce quick cybersecurity wins. In each section, you will learn about some of the key findings from Devolutions' SMB cybersecurity research as well as recommendations for how to effectively address the different problem areas to improve the security of your organization.

1. Implement Privileged Access Management

SMBs rely on privileged accounts to increase the efficiency and productivity of their employees. Unfortunately, hackers also rely on access to vulnerable privileged accounts to breach networks, access critical systems, and steal confidential data.

Privileged Access Management (PAM) refers to a class of solutions that help secure, control, manage, and monitor privileged access to critical assets. Devolutions' research has shown that 76% of SMBs do not have a fully deployed PAM solution in place, even though Gartner has identified the implementation of a PAM solution as one of its top 10 security priorities for 2019.

PAM solutions can detect and prevent access to highly privileged accounts. PAM solutions not only protect against external cyber threats, but they can also prevent insider threats like the accidental or deliberate misuse of privileged accounts. To counter these types of threats, PAM solutions provide you with the tools you need to restrict, revoke, and monitor access to highly privileged accounts.

However, many SMBs have been hesitant to adopt a PAM solution because they feel they can be too costly and too complicated. It is worth considering that a quality PAM solution can help streamline the management of privileged users and by reducing the time devoted to these tasks, this will free up resources to apply towards additional business objectives.

PAM solutions are an essential cybersecurity component and they can provide vital information about your privileged accounts that you might not be aware of. For instance, they can tell you how many privileged accounts you have that never expire or how many privileged accounts still exist that should have been deprovisioned.

PAM solutions provide special protection and monitoring of privileged accounts; when privileged accounts are created or defined, PAM tools provide unique protection for those credentials. A credential storage solution or password management system is utilized to securely store the privileged account authentication information that can prevent unauthorized access.

To access these privileged accounts, PAM users must utilize their PAM implementation for authentication. Each time these accounts are accessed, the PAM solution logs the session and tracks the actions performed. A complete record of the privileged account access includes the name of the user, what time their session began, how long it lasted, and the actions performed using those credentials.

The account types that PAM solutions enable SMBs to monitor and audit include:

- Domain Administrator Accounts
- Privileged User Accounts
- Local Administrator Accounts
- Emergency Access Accounts
- Application Accounts
- System Accounts
- Domain Service Accounts

To effectively serve the needs of the SMBs, PAM solutions need to provide ease of deployment and management, a secure password vault, logging and reporting, built-in two-factor authentication, account brokering, and role-based access to credentials. Ideally, the solution would not require any changes to Active Directory (AD) infrastructure and it should integrate with Azure AD.

2. Use a password manager to enforce strong password policies

Weak and reused passwords are two of the SMBs' biggest security exposures; research has shown that 81% of data breaches are caused by compromised, weak, and reused passwords. In addition, 29% of all breaches involve the use of stolen credentials; password misuse is a big cause of this.

Other studies have found that 59% of end users rely on the same passwords for all accounts. This is because users simply cannot remember all of the different passwords required to access the resources that they need. One recent survey showed business users must keep track of an average of 191 passwords. Further, they typically have to input their credentials for various websites and apps up to 154 times per month.

Password managers can significantly strengthen SMB cybersecurity by eliminating weak and reused passwords by enforcing strong password policies for the organization. Password managers also remove the burden of remembering and managing multiple passwords as they can store all the required authentication information in a secure, centrally controlled location. Password managers can automatically generate strong passwords for end users as well as restricting weak and forbidden passwords. They can also enforce several different password policies that ensure that your organization's passwords are secure. **The password policies provided by password managers should include:**

- Unique passwords – Prevents password reuse and requires each account has a different password.
- Minimum password length – Requires a minimum number of characters in a password.
- Complexity requirements – Ensures that the password can't contain the username and that it must use a combination of lowercase letters, uppercase letters, numbers, and symbols.
- Password history – Prevents old passwords from being reused for a specified period of time.
- Password age – Requires that a user must change their password in a specified time period.

A couple of other best practices for SMB password management are to use 2-factor authentication (2FA) when possible and to adopt the use of passphrases to create long passwords that can be more easily remembered. 2FA adds a level of security by requiring that the user presents something they have, like a FOB or keycard, in addition to something they know (a password). The use of passphrases makes passwords more difficult to break by increasing their length. In addition, SMBs should be sure to change all their passwords if there is evidence of a security breach.

While there are free password managers and alternatives like browser-based password vaults, there are restrictions when attempting to use these free and limited solutions.

Free offerings have no phone support, they can be difficult to deploy, have restricted feature sets, and typically

have no online backup. Using the browser to manage passwords is better than no password management at all, however, this also has several critical limitations for businesses.

First, the browser typically works for one person at a time and there is no ability to centrally secure or manage your passwords. More importantly, browser password management is extremely basic and it does not provide the password generation, complexity, and reuse rules that a real password manager provides. Browsers also only record passwords for websites which means that they are not able to work with other types of applications that the SMB may use.

3. Build your security strategy around the principle of least privilege

The principle of least privileged (POLP) essentially states that each process, user, or program, is only allowed to access just the information and resources that are necessary for its intended purposes. Unfortunately, many SMBs do not follow this principle. Instead, they often have users working with higher than needed permissions to make it easier for them to do their jobs. The downside to not using POLP is that this can open the door for cyberattacks; Devolutions' research has shown that 74% of data breaches are triggered by privileged credential abuse.

While using elevated privileges can make it easier to do some of the tasks, the risks involved far outweigh the benefits. Allowing users to work with administrative privileges significantly reduces the safeguards of other security frameworks.

For instance, if a user running elevated permissions clicks on an infected email link, it could install malware without being scanned by antivirus software or it could allow a hacker to locate and identify other vulnerabilities in your environment. This would not only impact the user's system, but it could also potentially impact other network systems as well as partner and customer data.

Implementing the principle of least privilege can minimize the organization's attack surface and stop cyberattacks and malware before they can seed in your environment. The first step toward implementing POLP is to analyze the current responsibilities and access levels for all of your users. As the name suggests, the default access should be the least required privileges. Any additional access should be granted only as needed.

Using role-based access can help you start to implement POLP. With role-based access, you assign users into different groups based on their job roles and then apply the appropriate privileges for those groups.

POLP ensures that end users are not commonly using highly privileged accounts which stops them from performing actions that could affect the entire environment or other networked systems; POLP can help contain

cybersecurity exploits and malware to a single user or device. But it is important to remember that POLP can work hand in hand with a PAM solution to limit, control, and monitor the use of privileged accounts – this is a best practice for helping to keep your systems secure.

4. Implement segregation of duties

SMBs should implement a Segregation of Duties (SoD) policy which separates administrator accounts from standard accounts as well as separating higher-level system functions from lower-level system functions. The goal behind a SoD policy is to reduce the opportunities for the unauthorized or unintentional misuse of organizational assets. SoD distributes the organization's duties between multiple employees.

The same factors that make SMBs vulnerable to external hackers also make them susceptible to attacks from disgruntled employees, ex-employees, contractors, and other rogue insiders. However, many smaller businesses think SoD is disruptive to end users because it can limit activities and reduce efficiency and productivity.

But implementing a strict SoD can help protect the SMB from both external hackers as well as insider threats and it is a basic step to hardening your internal controls. Security audits are a tool that can help enforce SoD but Devolutions' survey found that 62% of SMBs are not conducting yearly security audits and that 14% of SMBs never perform audits at all.

Regular security audits can expose and prevent possible SoD exceptions. It is best if the SMB can work with an external firm or consultant for their audits. However, many SMBs prefer to conduct inhouse audits because they are less costly and more convenient. In either case, using SoD will shore up security holes and can significantly streamline the auditing process.

5. Educate your users about cybersecurity

End users can be one of the biggest assets for security or they can be one of the biggest cybersecurity weaknesses. 79% of IT leaders believe that in the last 12 months, their own employees have accidentally put company data at risk.

To mitigate this problem, 88% of SMBs are providing some form of cybersecurity education to their end users. However, given the risks, the level of user education should be 100%.

For instance, susceptibility to phishing attacks is one clear area where user education can make a significant

impact. Research has found that 56% of IT decision-makers believe that preventing phishing attacks is their organization's number one cybersecurity priority. The same study revealed that 90% of cybersecurity breaches include a phishing element, and 94% of malware is delivered by email.

Training users not to open a suspicious email or to click on possible phishing links can be enough to prevent this entire attack mechanism.

Informed and conscientious users are the best defense against cybersecurity attacks. User education about the risks and best practices for cybersecurity can be one of the most comprehensive and costeffective defenses for SMB cybersecurity.

Informed users will know better than to open suspicious emails and attachments from unknown senders, they can implement safe password practices, and they will better adhere to the cybersecurity policies.

One of the most effective methods for the SMBs to promote user education is by enrolling users in online cybersecurity training. Online training is typically self-paced, and it can provide hands-on skillsbased threat detection and mitigation training. End users get immediate feedback on their progress and can move forward through the training based on their performance. Managers can also access the training platform to monitor their employees' progress.

Summary

SMBs cannot assume that their smaller size will protect them from cyberattacks. In fact, as you have learned in this whitepaper, the SMB is more vulnerable to cybersecurity attacks than larger organizations.

As the saying goes, it is not if these attacks are coming – it is when. Doing nothing can be disastrous and an SMB may not survive a cyberattack. By following the five quick SMB security wins presented in this whitepaper, you can step up your SMB security and stop most cyberattacks before they start.