Exploring PAM for SMBs

Devolutions

EVEN IF YOU DON'T BELIEVE YOUR BUSINESS IS A TARGET, YOU MIGHT BE COMPROMISED ANYWAY!

In this whitepaper, Devolutions explores the unique problems facing SMBs in securing privileged access.

IT professionals connect to remote systems to perform management tasks and often require administrative credentials. While some applications allow delegation so that tasks can be completed without a privileged account, many operations require administrative rights. Delegation also increases management costs as it requires businesses to determine whether applications support delegation, identify staff roles, the tasks that must be completed, and the rights required to perform the tasks. And this is an ongoing process as applications, systems, and roles change.

So, it's common for IT staff to be given administrative credentials to critical business systems to expedite access. In a worst-case scenario, it could be access to a shared administrative account. This often happens in Windows Server Active Directory, where the domain administrator password is widely known. But if the account is abused, falls into the wrong hands, or is otherwise compromised, it can result in a breach that might be difficult to recover from. In the case of Active Directory (AD), it's especially risky because AD is the identity management software that controls access to other business systems.

Assigning staff named user accounts with administrative privileges isn't much better because passwords are easily compromised. Insecure connections to remote systems or entering passwords on devices infected with malware are two common ways that passwords are discovered by hackers, using techniques that are automated to arbitrarily cast their virtual nets far and wide with minimum effort. Consequently, even if you don't believe your business is a target, you might be compromised anyway.

Administrative Credentials Increase Risk of Compromise

The proliferation of admin accounts used in any organization means that passwords are frequently stored in databases, spreadsheets, scripts, and other file types. But these can be easily compromised too. It is important to use a password manager or other secure vault to make sure that passwords are stored safely, can be retrieved when needed, and that passwords are not shared between different administrative accounts. Without a password manager, users tend to repeat the same password across multiple services, increasing the damage malicious actors can inflict when breaches do occur. Users also create weak passwords because without a password manager, it is difficult to remember long and complex passwords.

Windows Server provides granular permissions that allow organizations to assign users rights to perform functions without adding them to Administrators or other privileged groups. But this can lead to 'administrator-like' rights being assigned that if not carefully controlled, could result in a breach. Organizations also need to identify which rights are required to perform tasks. Windows PowerShell and Linux can be configured to restrict users to specific commands with elevated privileges. But this requires use of the command line or modern management tools, neither of which are common in SMBs.

Securely Managing Remote Access

There are several problems here that need to be addressed. When IT staff or third-party vendors access remote systems, they need not only the connection details - like IP address, DNS name, protocol, and other properties - but also privileged credentials to authenticate on the remote device.

Passwords and Multifactor Authentication

Using a password manager alone, organizations can ensure that strong passwords are in place for sensitive admin accounts. But users still need to enter passwords to connect. This can lead to password exposure if connections are insecure or if source devices are compromised. And passwords should be rotated to make sure that users can't get access to remote systems after they have performed the necessary changes.

Two-factor authentication (2FA) should be enabled for administrative accounts to provide extra security. Instead of just knowing a password, users must provide additional verification through something they have, like an authentication app on their smartphone. When 2FA is enabled, a compromised password isn't enough to log in.

Remote Desktop and Legacy Management Tools

Management tools rarely provide a way for organizations to monitor what changes are being made, which might result in unauthorized configuration changes that can't be traced. Systems should be secured and managed so that only sanctioned changes are allowed and that there is a log of all actions performed. Most system outages are the result of authorized changes. Servers that are subject to strict change control policies are easier to maintain and support because there is a known configuration that can be readily assessed and rolled back to a last known state if necessary.

Microsoft Remote Desktop (RDP) is the most common remote management tool in SMBs because it is easy to set up and configure. It provides access to a desktop environment and legacy GUI management tools that system administrators are familiar with. While RDP is convenient, it is prone to compromise if not configured correctly, especially when it is exposed to the Internet. Brute force and password spray attacks can give hackers an entry point into your network. Man-in-themiddle attacks, where users connect to an imposter device instead of the real server, can lead to credential and data compromise if RDP is not set up properly.

Privileged Access Management

Privileged access management (PAM) products solve the problems I outlined above by securing administrative credentials while allowing users to be productive. PAM lets organizations store and manage sensitive credentials in a centralized database. Instead of relying on manual processes, or even worse shared administrative accounts, PAM provides a secure vault and workflow to manage access to privileged credentials.

Users request access to passwords, which can be approved or denied. Much as document management systems like SharePoint let you check documents in and out, PAM lets you check passwords in and out to prevent them being used by more than one user concurrently. It's important to understand who is using an account, where, what is being done with it, and when. PAM logs all this information so that in the event of an incident, it's easy to get the forensics of a configuration change by running a report. Ideally, changes would be carried out using modern command-line shells or GUI tools, like Windows Admin Center, so that changes can be logged. But in practice, administrators usually perform tasks with tools that don't log changes. A good PAM solution can help establish the 'what' with session recording to capture exactly what actions were performed.

Devolutions Password Server

PAM solutions are generally designed with large enterprises in mind and most products are too complex for SMBs to implement and manage. That is if the price hasn't ruled out an enterprise PAM solution in the first place. For example, Microsoft's PAM solution requires two additional Active Directory forests and Microsoft Identity Manager (MIM). That's a lot of moving parts to manage and products to license.

Devolutions Password Server (DPS) is designed with SMBs in mind. It has a secure on-premises password vault that can be shared, and integrated privileged session management features to secure administrative accounts and access. DPS account brokering lets users and IT staff launch remote connections to servers, websites, and applications without ever needing to know the password of the account used. This alleviates the need for password rotation because passwords are never exposed to users. Regardless, DPS includes password rotation for those that would prefer to issue a different password every time access is requested.

DPS is managed via a web interface and access to it can be controlled using role-based access. Users connect to remote servers and applications using Devolutions Launcher. A lightweight desktop client for Windows, macOS, Linux, Android, and iOS, Launcher provides fast and secure access to remote services while DPS account brokering injects credentials without any user interaction. Brute force and password spray attacks can give hackers an entry point into your network. Man-inthe-middle attacks, where users connect to an imposter device instead of the real server, can lead to credential and data compromise if RDP is not set up properly.

Installing Devolutions Password Server

DPS is installed and set up using the Devolutions Password Server Console. It runs on all currently supported versions of Windows and Windows Server. DPS requires Internet Information Services (IIS) 7.0 or later and Microsoft SQL Server 2008 or later. SMBs that don't want to license SQL Server can use the free Express edition.

And while DPS is designed for SMBs, it supports several different deployment topologies for maximum flexibility. DPS and SQL Server can be installed on the same device for small deployments. For high availability, DPS can connect to a mirrored SQL Server failover cluster. DPS can also be configured for load balancing and set up in the cloud.

Passwords, Two-Factor Authentication, Encryption, and Service Integration Connections and credentials are stored in one or more centralized vaults protected by AES 256-bit encryption. Credentials can be checked in and out by authorized DPS operators so that users only get access to sensitive credentials when approval has been given. Quick access to websites is provided by the Devolutions Web Login browser extension and it can be used to generate strong passwords. Organizations with Devolutions Remote Desktop Manager can integrate DPS with third-party password managers like 1Password and LastPass.

DPS supports importing and synchronizing users and groups from Active Directory. And if AD is synchronized with Azure AD, Office 365 users can also be imported into DPS. There's built-in two-factor authentication for an additional layer of protection and the comprehensive and detailed reporting lets organizations track the who, what, when, and where. Furthermore, alerts can be set up to provide email notifications when a privileged account is used or changed.

Remote Desktop Manager

Devolutions Remote Desktop Manager (RDM) is a comprehensive toolset for IT staff to manage and share connections to remote systems. RDM stores passwords securely and performs account brokering so that IT staff can connect to remote devices without exposing privileged credentials. It integrates with DPS and Wayk to provide a complete remote access solution for IT professionals.

Helping IT professionals securely and efficiently connect to remote systems, RDM can store connections and credentials for Microsoft Remote Desktop (RDP), VNC, Hyper-V, Telnet, Citrix, VMWare, web, VPNs, SSH, FTP, and many other common protocols that are directly integrated into the product or available via addons. Account credentials can be stored directly in a user's session, a private password vault, or a shared database. RDM features include mobile access using the RDM Android or iOS app, secure offline access, and integrated command-line consoles.

While named user accounts are generally considered a best practice because they help organizations record who is accessing systems, RDM can simplify management with administrative password sharing. For example, instead of setting up named accounts for each user, RDM lets you use one admin account for all users. RDM records who accesses a system using a shared administrative account and reports other important information, like when and where connections are made, that might be required in an audit.

RDM stores connections in private or shared data sources, like Devolutions Password Server, SQL Server, DropBox, and many others. Connections can be shared over the Internet, intranet, or a private cloud. RDM Enterprise edition lets users securely share connections from a centralized repository and organizations can control access to privileged accounts using role-based access control (RBAC).

Next Steps

Devolutions Password Server is an enterprise-grade PAM solution designed to fit the needs of small and medium-sized businesses. Security breaches can be especially costly for SMBs because they aren't always able to absorb the impact of a serious attack. Managing access to privileged accounts is critical for ensuring system integrity and security. For a complete solution, DPS integrates with other Devolution tools that help IT manage remote connections.

For more information on Devolutions Password Server and Remote Desktop Manager visit https://devolutions.net/