Petri IT Knowledgebase BLOG SERIES

Guest Blog: Best Practices for Securing Remote Desktop Connections

Devolutions

THIS ARTICLE IS PART OF A BLOG SERIES CREATED BY THE PETRI IT KNOWLEDGEBASE TEAM AND TECHNICAL WRITER MICHEAL OTEY, IN PARTNERSHIP WITH DEVOLUTIONS.

Windows Remote Desktop Connection is one of the administrators most commonly used tools. It can provide remote desktop access to all the different Windows Server systems that are part of your local network or in the cloud. Properly securing your Remote Desktop Connections is vital because of the far-reaching access and capability that Remote Desktop Connection has. Enterprise solutions such as Devolutions Remote Desktop Manager can also help you secure and manage your Remote Desktop Connections. In this post, I'll cover some of the best practices for manually securing your Remote Desktop Connections.

Use Strong Passwords

Passwords are your first line of defense in securing your corporate infrastructure and that is just as true for Remote Desktop Connection as it is for your traditional desktop environment. All accounts with access to Remote Desktop Connections need to require strong passwords. You can require strong passwords in your domain using the Group Policy \Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy\Passwords must meet complexity requirements.

Don't Save Login Credentials in Your RDP Files

Saving your remote login credentials is a feature of Remote Desktop Connection that can make your connections to remote systems faster and easier by enabling you to log into the remote system by using the saved credentials. However, this can also be a potential security exposure because it bypasses the remote login. To always require a login to the remote system to edit the RDP file, click the General tab, then select the Always ask for credentials check box.

Limit Administrators Who Don't Need Remote Desktop

All administrators can use Remote Desktop Connection by default. However, if not all your administrators need access to Remote Desktop, then you should consider removing the Administrator account from RDP access. To do that you can use Administrative Tools to open Local Security Policy. Under Local Policies, open User Rights, then Allow logon through Remote Desktop Services. Remove the Administrators group. Then use the System control panel to add just the users and Administrators requiring Remote Desktop access to the Remote Desktop Users group.

Use Lockout Policies to Strengthen Password Protection

Using account lockout policies can also help strengthen Remote Desktop security. Account lockout policies enable you to prevent hackers or other unauthorized personnel from either guessing your passwords manually or from using automated password cracking tools by locking out the system for a specified period of time after a number of incorrect guesses. You can setup an account lockout policy by opening Administrative Tools, then Local Security Policy. Navigate to Account Policies and then open Account Lockout Policies. While the specific settings depend on the organization, consider setting Account lockout duration to three minutes, Account lockout threshold to five attempts, and Reset account lockout counter to three minutes as a starting point.

Take Advantage of Network Level Authentication

Network Level Authentication (NLA) is a more secure Remote Desktop Connection authentication method, as it provides a level of authentication before you establish an RDP session and the login screen appears. It uses fewer resources and can provide enhanced security by reducing your exposure to denial-of-service attacks.

NLA is enabled by default on Windows Server 2016, Windows Server 2012, Windows 8, and Windows 10. On Windows Server 2008 / R2 you can enable NLA by using Administrative Tools, then opening Remote Desktop Services and selecting Remote Desktop Session Host Configuration. Right-click the RDP-Tcp connection and select Properties from the pop-up menu. Use the General tab and then check the Allow connections only from computers running Remote Desktop with Network Level Authentication check box.