TWCA Risk Management Fund

Remote Desktop Protocol (RDP) Attacks

Remote Desktop Protocol (RDP), a Microsoft-developed network communications protocol that allows for the remote management of servers, desktops, terminal servers, and applications. RDP uses the standard network protocol Transmission Control Protocol/Internet Protocol (TCP/IP) to enable remote desktop access via port 3389. This allows users to interact with another computer’s interface through a secure, encrypted connection without physical cables like HDMI or USB. It can be efficient over Wi-Fi, ensuring users can gain access to their desktop environments from different locations. This makes it ideal for remote work. However, there is a vulnerability in some versions of RDP encryption that could allow unauthorized access to remote sessions. This type of vulnerability is exploited using what is called a man-in-the-middle attack. Think of this attack as similar to someone listening in on a phone conversation without either party knowing it.

RDP is widely used in networks for administration and remote work, and therefore wouldn’t be easy to stop its use. Here are some best practices when securing Remote Desktop Protocol.

1. **Use strong passwords.**
   Strong passwords on all accounts should be required for access to network resources, particularly RDP usage access.
2. **Use Two-factor authentication.**
   Organizations should consider using a two-factor authentication solution. RDP connections can be configured to integrate with multi-factor solutions such as Authenticator or Duo. The use of tokens and smart-cards can also be configured and provide two-factor security.
3. **Limit users who can log in using Remote Desktop.**
   Administrator accounts in Windows networks can log in to Remote Desktop. If you have multiple Administrator accounts on your network, you should limit remote access only to those accounts that need it. If Remote Desktop is not used for system administration, remove all administrative access via RDP, and only allow user accounts requiring RDP service.
4. **Update your software.**
   One advantage of using Remote Desktop as an admin tool is that components are updated automatically with the latest security fixes when the system is current with Microsoft. Ensure you are running the latest versions of both the client and server software by enabling and auditing automatic Microsoft Updates. If you are using Remote Desktop clients on other platforms, make sure they are still supported and that you have the latest versions. Older versions may not support high encryption and may have other security flaws.

5. **Restrict access using firewalls.**
   Use firewalls (both software and hardware where available) to restrict access to remote desktop listening ports (default is TCP 3389). Using an RDP Gateway is highly recommended for restricting RDP access to desktops and servers. VPN connection usage is also recommended for RDP.
6. **Set an account lockout policy.**
   By setting your computer to lock an account for a set number of incorrect guesses, you will help prevent hackers from using automated password guessing tools from gaining access to your system (this is known as a "brute-force" attack).
7. **Change the listening port for Remote Desktop.**
   Changing the listening port will help to "hide" Remote Desktop from hackers who are scanning the network for computers listening on the default Remote Desktop port (TCP 3389). Change the listening port from 3389 to something else and remember to update any firewall rules with the new port.

The TWCARMF Cyber Risk Services Advisor is ready to schedule Cyber Risk Assessments, Incident Response Plan Tabletop Testing visits, and Cyber Presentations for members. To get on the schedule, contact Lee Cain, Cyber Risk Services Advisor at (512) 619-1437, or Lee.Cain@sedgwick.com.