Courtesy of
CLG Insurance

CYBERRISKS&LIABILITIES

Preventing Ransomware Exposures From Remote Desk Protocol

Remote desk protocol (RDP)—which is a network communications protocol developed by Microsoft—consists of a digital interface that allows users to connect remotely to other servers or devices. Through RDP ports, users can easily access and operate these servers or devices from any location. RDP has become an increasingly useful business tool—permitting employees to retrieve files and applications stored on their organization's network while working from home, as well as giving IT departments the ability to identify and fix employees' technical problems remotely.

Unfortunately, RDP ports are also frequently being leveraged as a vector for launching ransomware attacks, which entail a cybercriminal deploying malicious software to compromise a device (or multiple devices) and demand a large payment be made before restoring the technology for the victim. In fact, a recent report from Kaspersky found that nearly 1.3 million RDP-based cyberattacks occur each day, with RDP reigning as the top attack vector for ransomware incidents.

Don't let RDP contribute to a costly ransomware incident for your organization. Review the following guidance to learn more about how ransomware attacks can occur via RDP and best practices for minimizing the likelihood of such an incident.

Ransomware Attacks via RDP

RDP-based ransomware attacks usually stem from organizations leaving their RDP ports exposed to the internet. Although doing so can seem more convenient for employers in the scope of remote work operations, internet-exposed RDP ports are easy for cybercriminals to identify and offer a clear access point for deploying harmful attacks.

The typical process of an RDP-based ransomware attack is as follows:

1. **Scanning**—First, a cybercriminal utilizes a port-scanning tool to search the internet for any exposed RDP ports. These scanning tools are often free and relatively simple to operate for attackers of varying skill levels.
2. **Gaining access**—After identifying an exposed RDP port, the cybercriminal then gains access to the targeted server or device by using stolen credentials. Attackers can secure these credentials by either purchasing them on the dark web or implementing a brute-force tool that can rapidly input a series of usernames and passwords until the correct combination is found.
3. **Disabling security features**—Once the cybercriminal has accessed the targeted server or device, they attempt to make it as defenseless against an attack as possible by disabling any existing security features (e.g., antivirus software, data encryption tools and system backup capabilities).
4. **Executing the attack**—From there, the cybercriminal is able to steal sensitive data and deploy a ransomware attack on a vulnerable server or device. Some attackers even install backdoors during this step to allow for easy access during future attacks.

Like other ransomware incidents, RDP-based attacks can result in devastating ramifications for the impacted organization—including business interruption issues, reputational damages and large-scale financial loss.

CLG
ACRISURE | AGENCY PARTNER

Strengthening RDP Against Ransomware

Although RDP-based ransomware attacks have become increasingly common, there are several ways for you to bolster your organization's RDP security and lessen the risk of such an incident impacting your operations. Consider the following best practices:

- **Close your RDP connection.** First and foremost, ensure that your RDP connection is not open to the internet.
- **Establish a virtual private network (VPN).** To keep your RDP port from being exposed to the internet, be sure to establish a VPN. This will allow remote employees to securely access your organization's RDP port, while also making the port far more difficult for cybercriminals to locate online.
- **Elevate authentication protocols.** Because cybercriminals require login credentials to properly execute an RDP-based ransomware attack, make sure you have effective user authentication protocols in place. Specifically, encourage employees to develop unique passwords for all of their devices and accounts. These passwords should be an appropriate length, refrain from using common words or phrases, and contain several special characters. In addition to strong passwords, consider requiring multifactor authentication for RDP port access as an extra layer of protection.
- **Implement login attempt limits.** To stop cybercriminals from being able to deploy brute-force tools to secure login credentials during an attack, update RDP port protection features to detect when multiple failed login attempts have occurred in a short period of time. Establish a limit on how many incorrect logins can occur before the user is blocked from further attempts—therefore halting an attack.
- **Utilize adequate security software.** Ensure all workplace technology is equipped with top-rated security software—including antivirus programs, a firewall, data encryption features and a gateway server—to deter attempted attacks. Update this software on a regular basis.
- **Restrict employee access.** Be sure to uphold the principle of least privilege by only providing employees with RDP access if they absolutely need it to conduct their work tasks. These employees should be trusted and trained in appropriate RDP usage. After all, granting extra employees unnecessary RDP permissions simply creates additional security gaps.
- **Have a plan.** Lastly, make sure your organization has an effective cyber incident response plan in place that addresses RDP-based ransomware attack scenarios. This plan should promote the backup storage of any critical data in multiple secure locations (both on-site and off-site) to minimize potential losses. Practice this plan regularly with staff and make updates as needed.

For additional risk management guidance and insurance solutions, contact us today.