Remote Desktop Protocol

What is RDP and why does it matter?

Remote Desktop Protocol (RDP) is a server connection provided by Microsoft and other operating systems that allows users to remotely connect to other computers over a network.

The rise of remote work has created new opportunities for cyber criminals to exploit open RDP ports. More than 3.5 million internet-connected devices had an externally facing RDP port as of November 2020.[1] Additionally, more than 50% of all ransomware attacks in Q4 of 2020 were attributable to compromised RDP.[2]

An open RDP port is the biggest ransomware attack vulnerability for most businesses.

Now, here's the good news: Open RDP ports are typically an easy fix. The key is identifying threats and closing RDP ports before they're exploited in a cyber attack.

How At-Bay helps keep businesses secure

We conduct a sophisticated security scan of every business we quote to look for vulnerabilities, like open RDP ports. And because cyber risk is dynamic and constantly evolving, we deploy our active risk monitoring technology to continuously scan for cyber threats throughout the life of every policy.

Our proactive approach to risk management has proven to be one of the most effective ways to reduce ransomware attacks. We're constantly on the lookout for cyber threats, and our results speak volumes.

At-Bay's ransomware claims frequency is 5x lower than the industry average.

What happens if At-Bay detects a vulnerability?

If an open RDP port is identified at the time of quoting, we provide recommendations to quickly and securely address the vulnerability. If we detect a new vulnerability during a policy period, we immediately alert both the insured business and their broker about the issue.

When necessary, we provide recommendations to the insured business' technical team on how to resolve the issue while maintaining functionality in a secure manner. If an open RDP is required for business operations, we recommend hiding the RDP behind a secure gateway, such as a virtual private network (VPN), and enabling network-level authentication.

[1] CIS: Center for Internet Security issues new remote desktop security guide, based on CIS Controls

[2] Coveware: Ransomware Costs Double in Q4 as Ryuk, Sodinokibi Proliferate

This document is intended for information purposes only and does not modify or invalidate any of the provisions, exclusions, terms or conditions of the policy and endorsements. For specific terms and conditions, please refer to the coverage form. ©2022 At-Bay. All Rights Reserved.