RDP چیست و آیا می‌توان RDP را ایمن کرد؟

پروتکل دسکتاپ از راه دور (RDP) یک پروتکل ارتباطی شبکه‌ای است که توسط مایکروسافت ایجادشده و به کاربران اجازه می‌دهد از یک مکان راه دور به رایانه دیگری متصل شوند. این‌یک افزونه از پروتکل‌های ارتباطی نقطه‌به‌نقطه T.120 است که توسط ITU (اتحادیه بین‌المللی مخابرات) استانداردشده است.

RDP یک رابط گرافیکی برای اتصال از راه دور یک کامپیوتر به کامپیوتر دیگر فراهم می‌کند، برای استفاده از RDP کاربر مبدأ باید از رایانه‌ای استفاده کند که نرم‌افزار کلاینت RDP را نصب‌کرده و کار می‌کند. رایانه‌ای که کاربر می‌خواهد به آن دسترسی پیدا کند باید از نرم‌افزار سرور RDP استفاده کند که به مشتری امکان اتصال از راه دور را می‌دهد، پس از اتصال کاربر ایجادکننده درخواست می‌تواند دسکتاپ رایانه‌ای را که از طریق RDP به آن متصل می‌شود ببیند و به برنامه‌ها و داده‌های روی آن دسکتاپ دسترسی داشته باشد. شناخته‌شده‌ترین نرم‌افزار مخصوص سمت مشتری RDPنرم‌افزار ارائه‌شده توسط مایکروسافت است که در حال حاضر «Remote Desktop Connection» نامیده می‌شود. این نرم‌افزار قبلاً «Terminal Services Client» نامیده می‌شد، نامی که ممکن است هنوز در برخی منابع قدیمی در این زمینه یافت شود.

هنگامی‌که دستگاهی دارای نرم‌افزار مشتری است که از RDP استفاده می‌کند، کاربر می‌تواند به هر رایانه‌ای که دارای ویندوز یا سیستم‌عامل سازگار دیگری است متصل شود. یک کلاینت منبع باز به نام rdesktopکه از طریق خط فرمان اجرا می‌شود نیز در

دسترس است، نرم‌افزارهای مخصوص کاربران با رابط کاربری گرافیکی متعددی هم در دسترس هستند که بر اساس عملکرد ارائه‌شده توسط rdesktop ساخته‌شده‌اند، مایکروسافت علاوه بر استفاده از این پروتکل برای دسترسی به رایانه‌های راه دور، در راهکارهای محاسبات ابری Azure خود از RDP برای ارائه رایانه‌های مجازی به کاربران استفاده می‌کند.

با RDP می‌توانید با استفاده از دستگاهی باقابلیت کمتر در خانه یا در جاده به یک ایستگاه کاری قدرتمند در دفتر دسترسی داشته باشید، با این قابلیت می‌توانید با در اختیار داشتن یک سیستم کامپیوتری ضعیف و برقراری ارتباط آن با یک سیستم قدرتمند از عملکرد بالای سیستم قوی‌تر بهره‌مند شوید، با این حال این پروتکل با بسیاری از مسائل امنیتی شناخته‌شده مواجه است، این آسیب‌پذیری‌ها همراه با پایگاه کاربری عظیم RDP آن را به یک هدف محبوب برای هکرها تبدیل می‌کند، استفاده از RDP در راهکار رایانش ابری مایکروسافت آن را برای مجرمان سایبری که به دنبال سوءاستفاده از آسیب‌پذیری‌ها هستند جذاب‌تر می‌کند.

پورت‌های باز مانند پورت‌های مورداستفاده در RDP هدف جذابی برای مجرمان سایبری هستند، کاربران اغلب یا از گذرواژه‌ها استفاده چندباره می‌کنند یا گذرواژه‌های ساده و آسان برای به خاطر سپردن را انتخاب می‌کنند که به‌راحتی با یک حمله سایبری شکسته می‌شوند. افزایش استفاده از RDP مرتبط با افزایش ناشی از کرونا در کار از راه دور منجر به افزایش شدید حملات سایبری که پورت‌های RDP را هدف قرار می‌دهند شد. حملات RDP در سال ۲۰۲۱ بسیار زیاد بود به‌طور مثال در ماه مه ۲۰۱۹ وصله‌ای برای رفع آسیب‌پذیری مهم به نامBlueKeep منتشر شد که امکان اجرای کد از راه دور را فراهم می‌کرد، به گفته مایکروسافت این آسیب‌پذیری worm بود، به این معنی که می‌توانست خود-منتشر باشد که می‌توانست مشکلات گسترده‌ای ایجاد کند، یا نسخه ۶.۱ می‌تواند تمام نام‌های کاربری و تصاویر کاربران را در سرورهای RDP نشان دهد، در مارس ۲۰۱۲ نیز یک آسیب‌پذیری که با یک به‌روزرسانی امنیتی حیاتی برطرف شد می‌توانست رایانه‌ها را توسط کرم‌ها و کلاینت‌های احراز هویت نشده در معرض خطر قرار دهد. نسخه ۵.۲ در برابر حملاتman-in-the-middle آسیب‌پذیر بود و در این حالت هکر می‌توانستند ارتباطات را استراق سمع کرده یا بدزدند.

حال آیا می‌توان RDP را ایمن کرد؟

کارشناسان امنیتی توصیه می‌کنند که کاربران و مدیران اقدامات احتیاطی زیر را برای افزایش امنیت استفاده از RDP خود انجام دهند :

v. از پروتکل‌های رمز عبور قوی پیروی کنید، مجوز تائید هویت چندعاملی را فعال کنید و سیاست‌های قفل‌کردن را برای جلوگیری از حملات brute force اعمال کنید.

v. پورت‌های RDP را پشت فایروال قرار دهید که فقط با استفاده از VPN قابل‌دسترسی است.

v. اجازه ندهید از RDP برای حساب‌های سرپرست استفاده شود.

v. میزبان‌های خاص مورد اعتماد را در لیست سفید قرار دهید.
vi. وقتی از RDP استفاده نمی‌شود، پورت‌هایی را که استفاده می‌کند ایمن کنید.

v. به‌روزرسانی‌های خودکار را برای نرم‌افزار کلاینت/سروری که استفاده می‌کنید فعال کنید تا مطمئن شوید که همیشه آخرین نسخه را دارید

که در آن آسیب‌پذیری‌های امنیتی شناخته‌شده، برطرف شده است.

البته که درنهایت برخی متخصصان امنیتی معتقد هستند بهترین راه برای ایمن نگه‌داشتن RDP این است که به‌هیچ وجه از RDP استفاده نکنید و در عوض از مکانیزم اتصال دسکتاپ از راه دور متفاوتی را که ذاتاً ایمن‌تر است انتخاب کنید.

- روش‌های دسترسی از راه دور جایگزین امن‌تر، امکان دسترسی و استفاده از دسکتاپ‌های راه دور را بدون تکیه‌بر پروتکل RDP فراهم می‌کنند. به دنبال راهکاری باشید که از احراز هویت چندعاملی (MFA) و همچنین ویژگی‌های امنیتی ازجمله مدیریت مبتنی بر نقش، دسترسی در سطح گروه و مدیریت خط‌مشی و SSO (SAML و oAuth) پشتیبانی می‌کند و ترافیک بین کلاینت‌ها و ترمینال سرورها را حتی در سراسر شبکه‌های عمومی به‌طور کامل رمزگذاری می‌کند. کاربران راه دور باید با استفاده از مدیریت هویت و دسترسی احراز هویت شوند. پس از احراز هویت، دسترسی آن‌ها باید فقط به برنامه‌ها و دستگاه‌های متصل به شبکه و دسکتاپ داخلی خود که صراحتاً مجاز به استفاده از آن‌ها هستند محدود شود.

منبع:

https://www.ericom.com/glossary/what-is-rdp