امنیت در اتصال به سیستم از راه دور

امنیت در اتصال به سیستم از راه دور

تاریخ تنظیم : اردیبهشت ۱۳۹۸

گروه شرکت‌های شاتل

فهرست مطالب

سیستم اتصال از راه دور تا چه اندازی ایمن است؟

اتصال از راه دور، در اصل بر روی یک کانال رمزگذاری شده عمل می‌کند و مانع ورود افراد دیگر از طریق گوش فرا دادن به شبکه می‌شود. بااین‌حال در نسخه‌های قبلی RDP حفره‌های قابل‌نفوذی نیز وجود دارد. به‌عنوان‌مثال یک فرد می‌تواند با استفاده از متد man-in-the-middle در ارتباط شما نفوذ کند.

برای جلوگیری از این کار می‌توان از ارتباط از طریق SSL/TLS در ویندوز ویستا، Seven، و سرور ۲۰۰۸/ ۲۰۰۳ و سرورهای جدیدتر استفاده کرد.

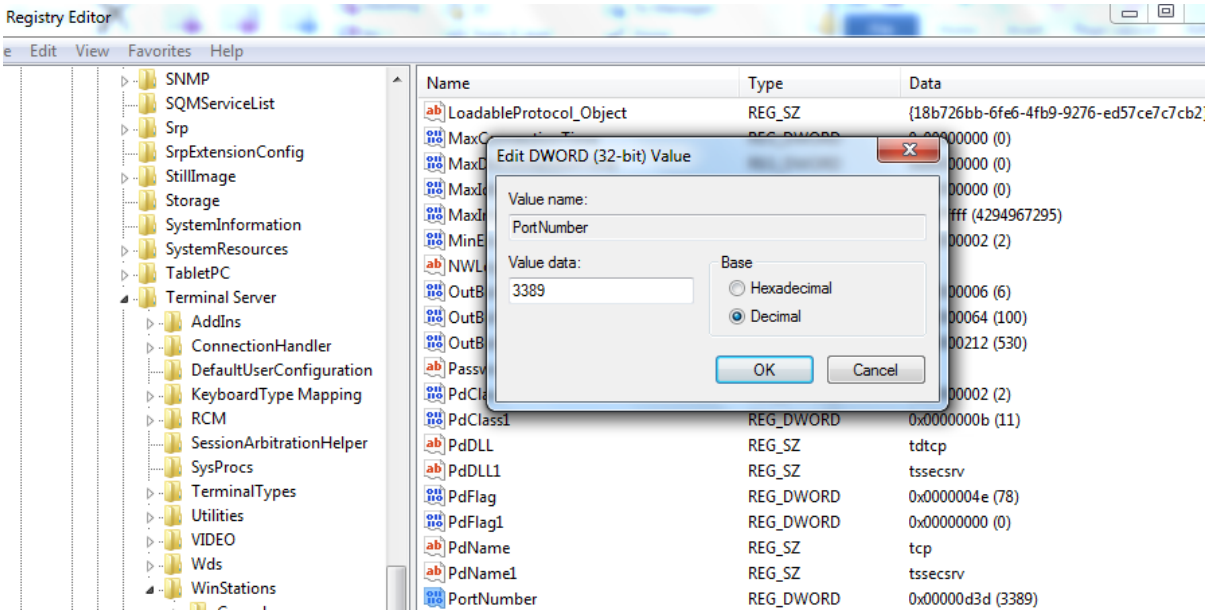
باوجوداینکه استفاده از RDP بسیار امن‌تر از باقی ابزارها به‌مانند VNC ست (به دلیل رمزگذاری ارتباط) بازهم خطراتی دراین‌ارتباط وجود دارد که می‌بایست با رعایت آن‌ها از خطرات احتمالی جلوگیری کنیم.

پورت مربوط به RDP را تغییر دهید

به‌صورت پیش‌فرض پورتی که برای استفاده از ارتباط از راه دور استفاده می‌شود پورت ۳۳۸۹ است.

شما می‌توانید در Registry ویندوز خود این پورت را به پورت دیگری تغییر دهید.

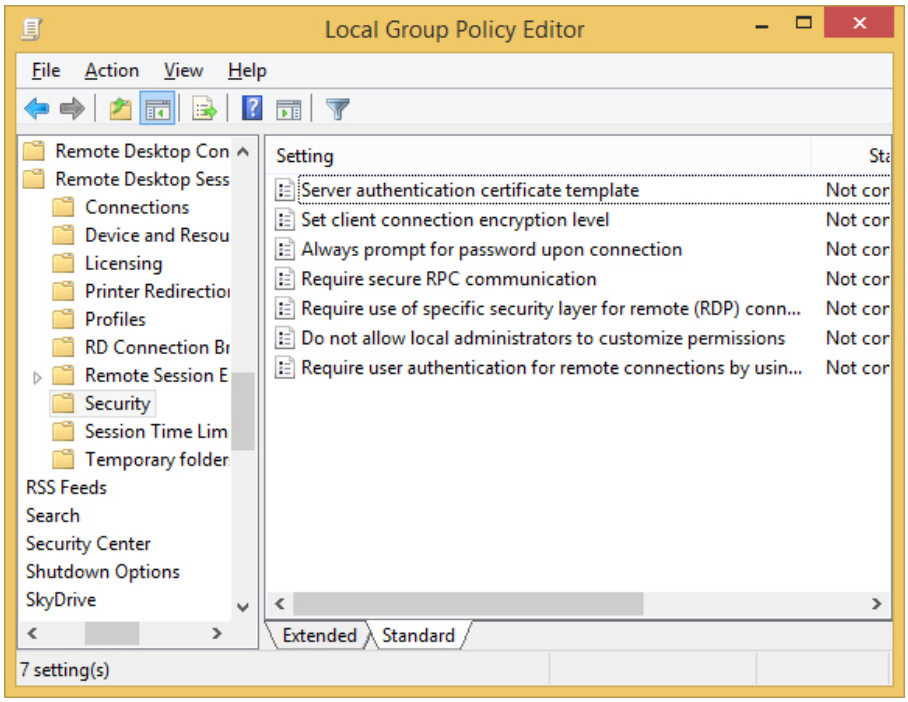
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\
PortNumber



شکل ۱

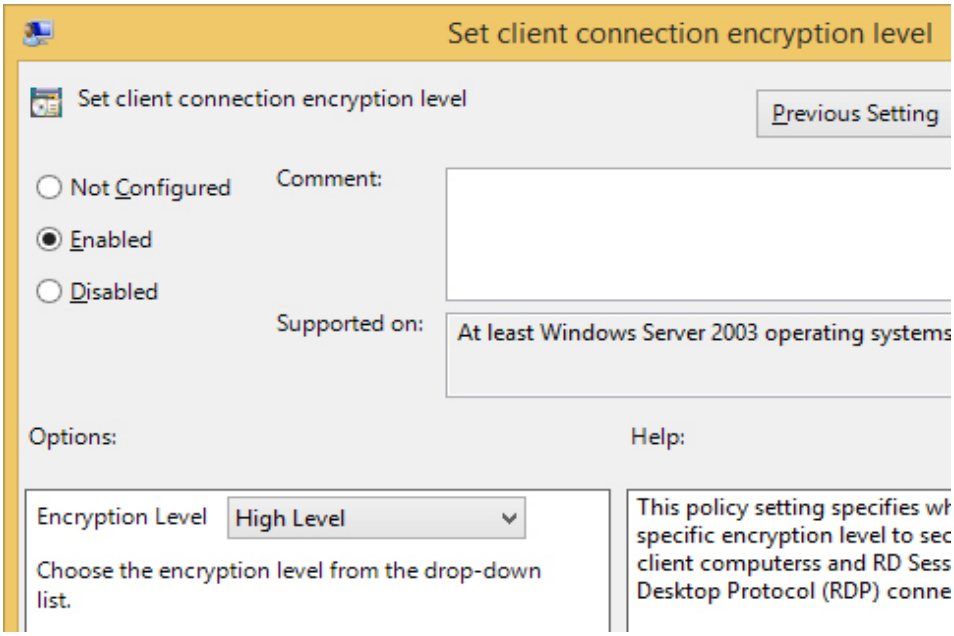
Encryption Level مربوط به سرویس Remote را افزایش دهید

شما می‌توانید میزان امنیت Remote Desktop خود را از همین Registry تغییر دهید :



شکل ۲

با انتخاب Server authentication certificate template این گزینه را Enable و در بالاترین سطح امنیت قرار دهید :



شکل ۳

اطمینان حاصل کنید که نیاز است از این سرویس استفاده کنید؟

در شبکه خود جست‌وجو کنید که این پورت باز است یا خیر؟

برای این کار می‌توانید از قابلیت Telnet و یا سایت‌هایی که برای چک کردن باز بودن پورت هستند استفاده کنید.

درصورتی‌که این پورت در شبکه شما باز است اما از دلیل باز بودن آن اطلاع ندارید، حتما سیستم مربوطه را بیابید و این سرویس را غیرفعال کنید.

از سرویس RDP Gateway استفاده کنید

استفاده از سرور RDP Gateway این اجازه را به شما می‌دهد که کلیه دسترسی‌های Remote را از روی یک سیستم به‌عنوان سرور انجام دهید.

در این سرور تمامی درخواست‌ها از طریق پورت ۴۴۳ دریافت شده و به سیستم‌های مقصد تحویل می‌دهد.

از SSH یا IPsec برای اتصال از راه دور استفاده کنید.

شما می‌توانید با استفاده از یک‌لایه اضافی برای شناسایی هویت از طریق SSH و یا IPsec امنیت بیشتری برای ارتباط خود فراهم کنید.

از به‌روز بودن نرم‌افزارهای مربوط به اتصال از راه دور اطمینان حاصل کنید

یکی از مواردی که حتما می‌بایست در نظر داشته باشید استفاده از آخرین نسخه‌های موجود برای اتصال از راه دور است.

شرکت مایکروسافت به‌صورت مداوم در حال به‌روزرسانی سیستم ریموت خود است. برای این مورد فقط باید مطمئن باشید که به‌روزرسانی دستگاهتان فعال باشد.

هم‌چنین در صورت استفاده از دیگر سیستم‌عامل‌ها ، اطمینان حاصل کنید که نرم‌افزارهای مورداستفاده به‌روزرسانی شده و هنوز پشتیبانی می‌شوند. نسخه‌های قدیمی‌تر ممکن است رمزگذاری صحیحی را پشتیبانی نکرده و دارای نقص امنیتی باشد.

از رمزهای با پیچیدگی بالا برای اشخاصی که به ریموت سیستم دسترسی دارند استفاده کنید

سعی کنید که دسترسی Remote Desktop را به هر شخصی می‌دهید اطمینان حاصل کنید که از رمزهای عبور با پیچیدگی‌های کافی استفاده کنند.

دسترسی‌ها را با استفاده از فایروال‌های سیستم، مودم و ... محدود کنید

در حال حاضر فایروال‌های سخت‌افزاری و نرم‌افزاری بسیاری برای محدود کردن دسترسی از طریق پورت‌های مختلف وجود دارد.

سعی کنید با استفاده از این فایروال‌ها ، دسترسی‌های موجود به‌غیراز سیستم و پورت‌های مشخص را محدود کنید.

این فایروال بر روی مودم‌ها، دستگاه‌های میکرو تیک ، نرم‌افزارها و سخت‌افزارهایی وجود دارد.

مهم‌ترین گزینه در تعریف فایروال تعریف صحیح از Source ، Destination و پورت است.

Network Level Authentication را فعال‌سازی کنید

استفاده از قابلیت Network Level Authentication در ویندوز ویستا ، ۷ و سرور ۲۰۰۸ می‌تواند سطح بالاتری از امنیت را ایجاد کند. در این روش یک سطح اضافی برای احراز هویت نیز مشخص می‌شود.

فقط باید در نظر داشت که سایر سیستم‌عامل‌ها به‌جز ویندوز از این قابلیت پشتیبانی نمی‌کند.

کاربرانی که می‌توانند از Remote Desktop استفاده کنند را محدود کنید

به‌صورت پیش‌فرض کلیه Administrator ها جزو گروه Remote Desktop هستند.برای جلوگیری از ایجاد مشکل سعی کنید این دسترسی را فقط به افرادی که می‌بایست از این قابلیت استفاده کنند محدود کنید.

یک سیاست برای Lock شدن ورودهای ناموفق مشخص کنید

شما می‌توانید مشخص کنید که در زمان ورود به سیستم و اشتباه واردکردن پسورد ، چه سیاستی پیش‌گرفته شود.

به‌عنوان‌مثال با سه بار سعی ، سیستم Lock شده و به مدت سه دقیقه Lock باقی بماند.

برای انجام این کار می‌بایست وارد قسمت زیر شوید :

Start-->Programs-->Administrative Tools-->Local Security Policy
Account Policies-->Account Lockout