توصیه‌های امن‌سازی RDP

با توجه به گزارشات متعدد از حمله باج افزارها به سرورهای ویندوزی از طریق سرویس RDP در کشور از اسفند ۹۵ تاکنون و پیرو اطلاعیه های قبلی مرکز ماهر در این خصوص، لازم است راهبران شبکه نسبت به امن سازی جدی سرورهای خود اقدامات لازم را به عمل آورند.

بدین منظور درصورت عدم نیاز، این سرویس را غیرفعال نموده یا دسترسی به آن را محدود به آدرس‌های IP خاص نمایند. در ادامه توصیه‌هایی درخصوص امن‌سازی این سرویس ارائه شده است.

برای کنترل و مدیریت یک کامپیوتر از راه دور می‌توان از برنامه‌های مبتنی بر پروتکل Remote Desktop استفاده کرد. در سیستم عامل‌های مبتنی بر Microsoft Windows از نرم‌افزار پیش‌فرض Remote Desktop Client استفاده می‌شود که بایستی برای استفاده آن بر بستر اینترنت چندین مشخصه آن را امن‌سازی نمود تا از دسترسی به آن توسط افراد غیرمجاز جلوگیری شود.

نکاتی که در ذیل معرفی شده، اهم موارد امن‌سازی مطرح در استاندارد NIST-SP800-46r2 می‌باشد که بایستی برای احراز امنیت در ارتباطات راه دور Remote Desktop مورد ارزیابی واقع شود.

- فعال‌سازی Encryption بعد از پروسه Authentication
- عدم استفاده از Encryption های ضعیف
- استفاده از روش‌های احراز اصالت چند عاملی توسط کلمه عبور، توکن، PKI، ...

- استفاده از سیستم‌عامل‌های امن برای سیستم‌های Server (همچون OpenBSD) که اجازه نصب انواع KeyLogger ها را نمی‌دهند.
- در بسیاری از ارتباطات Remote Desktop قابلیت دسترسی به درایوهای کامپیوتر راه دور (Server) توسط Map نمودن درایوها در نسخه Client به‌صورت پیش‌فرض فعال می‌باشد و بایستی در اکثر موارد که نیازی به چنین قابلیتی نیست آن را غیر فعال نمود.
- غیر فعال نمودن Printer های مجازی همچون انواع PDF Generator ها روی سیستم Server
- غیر فعال نمودن عملگر Paste از روی Clipboard
- غیر فعال نمودن ScreenShot برای کلاینت‌ها برای جلوگیری از دسترسی بسیاری از Malware ها همچون Zeus به اطلاعات Clipboard و تغییر محتوا یا دسترسی به قسمت‌های حفاظت شده حافظه.
- درنظر گرفتن حداقل سطح دسترسی برای کاربران Remote Desktop تا حدی که کاربر نتواند فعالیت‌های خاص مدیر را انجام دهد. از جمله عدم دسترسی به تنظیمات Sharing یا تعریف کاربران جدید و یا دسترسی مستقیم به درایوهای سیستمی ویندوز (C:\) ویا فولدرهای حاوی مشخصات کاربری (C:\Users) و صد البته عدم توانایی اجرای محیط CMD
- به‌روز نگهداری نسخه سیستم عامل و همچنین به‌روزنگهداری Patch های سیستم عامل Server
- به‌روزرسانی مداوم آنتی ویروس نصب شده روی سیستم Server
- اطمینان از عدم دسترسی کاربر RDP به پنل مدیریتی AntiVirus یا Firewall.

- شخصی‌سازی قوانین مربوط به ترافیک های Inbound و Outbound در Firewall نصب شده روی سیستم Server.
- اطمینان از عدم نصب برنامه‌های غیر لازم روی سیستم عامل Server.
- استفاده از کلمات عبور مستحکم و غیر قابل حدس و حتی الامکان Random که به‌صورت مداوم تغییر کنند.
- محافظت از Remote Desktop Server به‌وسیله یک VPN Server حاوی کلیدهای سفارشی‌سازی شده PKI
- اطمینان از عدم هرگونه Route غیر لازم بین VPN و سایر Interface ها.
- اطمینان از عدم دسترسی کاربر RDP به Page فایل‌های سیستم عامل جهت جلوگیری از نشت اطلاعات حیاتی سیستم عامل.
- انجام ندادن هرگونه Hibernating یا Suspend در سیستم عامل Server جهت جلوگیری از احتمال باقی ماندن اطلاعات کاربران بر روی حافظه.