IT & Security Consultores Ltda.
NIT 811.031.833-3
*Soluciones Antivirus Multinivel *Consultoría en Seguridad Informática
*Recuperación Avanzada de Datos *Mantenimiento Integrado de Software y Hardware
*Soporte Técnico y Capacitación

LOS PELIGROS DE PUBLICAR EL SERVICIO DE ESCRITORIO REMOTO

Calle 37 No 79-17 Laureles Tels. 604 45 41 Ext. 203
Medellín – Colombia E-mail: mvargas@its-consultores.com

EL SERVICIO DE ESCRITORIO REMOTO

El servicio de escritorio remoto es uno de los más importantes que se usan en una red empresarial, ya que permite acceder desde un equipo a otro, de manera total y directa. Normalmente en las empresas se usa el escritorio remoto para que los usuarios dentro de la red puedan conectarse a algún servidor interno, sin embargo usualmente también se utiliza este servicio para que usuarios en el exterior de la red puedan conectarse remotamente a algún servidor adentro de la empresa.

Lamentablemente, así como este servicio tan importante nos facilita la vida al permitirnos conectar a otro equipo, también implica el riesgo inherente de que sea usado para que alguien no autorizado se conecte indebidamente a un equipo o servidor, y aunque este servicio maneja autenticación, es decir que el usuario para conectarse tiene que autenticarse con un usuario y contraseña válidos, esto no siempre es suficiente para que no pueda ser usado por cibercriminales.

LOS PELIGROS DE PUBLICAR EL SERVICIO DE ESCRITORIO REMOTO

La principal razón por la que hacemos este boletín con este tema es porque cada vez es más común para nosotros atender casos de empresas víctimas de ransomware que se infectan por tener un servidor con el escritorio remoto publicado, precisamente podríamos decir que hoy en día ese es el mayor riesgo que implica, porque es lo que normalmente buscan los cibercriminales al vulnerar el escritorio remoto de algún servidor.

¿Cómo lo hacen? Es muy simple, los cibercriminales tienen herramientas que les permite realizar sondeos por todo internet, a la gran mayoría de direcciones IP públicas, con estos sondeos lo que consiguen es encontrar qué direcciones IP tienen puertos abiertos escuchando, además para optimizar el tiempo de sondeo normalmente lo enfocan en puertos específicos de servicios importantes como páginas web (80 y 443), correo electrónico (25), SSH (22), FTP (21) y el escritorio remoto de Windows que funciona nativamente por el puerto 3389.

Luego de que los cibercriminales encuentran algún servidor con estos puertos abiertos y escuchando, proceden a atacar dichos servicios, en el caso de que encuentren un servidor con el escritorio remoto publicado, proceden a realizar distintos tipos de ataques que van desde explotar alguna vulnerabilidad de Windows que pueda tener dicho escritorio remoto, hasta realizar un ataque de fuerza bruta que tarde o temprano les permita acertar con la clave del administrador, todo esto con el objetivo final de conseguir acceso al servidor y posteriormente infectarlo.

¿QUÉ MEDIDAS DE SEGURIDAD SE PUEDEN TOMAR SI TENGO QUE PUBLICAR UN ESCRITORIO REMOTO?

Es normal que una empresa tenga la necesidad de acceder desde una red externa a un escritorio remoto de un equipo en la red interna, por eso daremos algunas recomendaciones para suplir esta necesidad:

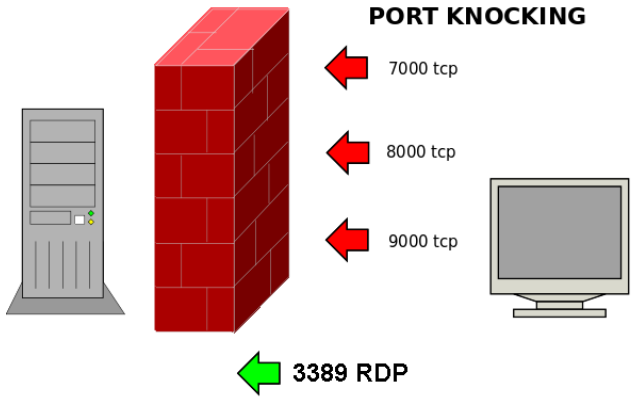
1. Utilizar una VPN: La mejor alternativa para evitar los riesgos de publicar un escritorio remoto y casi cualquier servicio en general, es crear una VPN que permita conectarse al escritorio remoto de algún servidor, por lo tanto el que lo quiera hacer, tendrá que conectarse primero a dicha VPN.

2. Cambiar el puerto estándar: El puerto por defecto del servicio de escritorio remoto es el 3389, por lo tanto los sondeos y ataques de los cibercriminales normalmente irán enfocados a ese puerto. Precisamente una buena medida de seguridad es enmascarar este puerto, lo cual consiste en publicar el RDP mediante un puerto distinto al 3389.

3. Deshabilitar el acceso al usuario Administrador: Este usuario es al que normalmente intentarán vulnerar mediante ataques de fuerza bruta, lo mejor es que el acceso se realice mediante otro usuario.

4. Trusted Host: Esto es una característica que nos permite definir qué direcciones IP son las que tendrán permitido iniciar la conexión a un servicio en específico, el RDP de Windows no cuenta directamente con esta característica incorporada pero mediante el firewall de Windows si se pueden establecer dichas reglas, adicionalmente desde el mismo firewall perimetral con el que se publica el servicio, se debe poder también establecer que la publicación se realice únicamente para direcciones IP específicas, lo que garantiza que el servicio no quede expuesto a todo internet.

5. Port Knocking: Este es un mecanismo de seguridad avanzado que permite que se pueda acceder a un servicio en un puerto en específico solamente si se han realizado peticiones a una secuencia determinada de puertos, por ejemplo puedo activar este mecanismo para que un usuario pueda acceder al RDP en el puerto 3389 únicamente si ha realizado primero peticiones al puerto 300, 301 y 302 consecutivamente, sino simplemente no le responde el servicio RDP.



Enlaces de interés con información más detallada

- Ransomware a través de escritorio remoto
https://www.esecurityplanet.com/threats/new-attacks-spread-ransomware-via-remote-desktop-protocol.html

- Como asegurar el servicio de escritorio remoto y cambiar el puerto de uso
https://www.howtogeek.com/175087/how-to-enable-and-secure-remote-desktop-on-windows/

- Port Knocking
https://es.wikipedia.org/wiki/Golpeo_de_puertos