

PROBLEMAS DE SEGURIDAD ASOCIADOS AL ACCESO REMOTO

Autor: Rodrigo Ferrer CISSP

SISTESEG

Bogotá

Colombia

Hoy en día quizás impulsado por el desarrollo de las tecnologías de la información tales como: Internet, Ethernet de alta velocidad, HTTP, XML, IPV6, Intranets, entre otras, muchas entidades permitirían como posibilidad el poseer sistemas de acceso remoto a su información, es decir, que no es suficiente con que la información esté almacenada en servidores diseñados para esta labor, si no, que es también indispensable hacer llegar a usuarios remotos o externos a una determinada red esta información, con el fin de ser procesada, modificada o actualizada según que las circunstancias y las necesidades así lo determinen. Así planteado, es claro la necesidad, pero no basta sólo con ella, ni con la tecnología que la podría soportar, si no que dado la presencia de amenazas sobre la seguridad de la información en las redes hoy existentes, es necesario e inevitable que este proceso de permitir el acceso a la información de modo remoto, en realidad sea parte de una decisión estratégica que contemple entre otros aspectos el tema de seguridad de la información, como estrategia fundamental.

Pudiera parecer que este aspecto de considerar en todo proyecto de acceso remoto el tema de la seguridad de la información, es uno de los tantos aspectos que se deberían considerar, al lado de por ejemplo las tecnologías a utilizar, velocidades de conexiones y el tema de privilegios de usuarios sobre los recursos a acceder. Pero en lo que queremos insistir es que la seguridad de la información dentro de un proyecto de acceso remoto es uno de los aspectos críticos y fundamentales, que sin ellos, sería un riesgo demasiado alto el intentar acometer este tipo de tecnologías para el acceso de la información.

Hoy en día la información según por ejemplo ISO 17799/ISO 27001, es considerada uno de los activos más importantes de la organización y por lo tanto es indispensable que en todo proyecto que pudiera cambiar las condiciones técnicas de una infraestructura de información, se tomen las medidas preventivas, detectivas y correctivas con el fin de poder garantizar la confidencialidad, la integridad y la disponibilidad de la información.

Con lo anterior, se trata pues, que en todo proyecto de acceso remoto siempre tengamos en cuenta que paralelamente a él, debe correr un proyecto de control del acceso a la información. Este control de acceso considera múltiples niveles dentro de un sistema de información, a saber:

- ✚ Control de acceso a la información
- ✚ Control de acceso a las bases de datos
- ✚ Control de acceso a la aplicaciones(aplicación web)
- ✚ Control de acceso en el sistema operativo
- ✚ Control de acceso a un sistema de directorios
- ✚ Control de acceso a la red interna
- ✚ Control de acceso a la red WAN
- ✚ Control de acceso a la DMZ o firewall
- ✚ Control de acceso físico

Es bien sabido, que el nivel de seguridad de acceso total depende directamente del nivel más bajo de seguridad que tengamos en estos controles que hemos mencionada anteriormente. Es decir, que el proyecto de acceso remoto debe considerar todas las variables antes mencionadas que son obviamente controles de tipo lógico y físico, pero aun no es suficiente, ya que se debe complementar esta estrategia con controles administrativos como procedimientos para el acceso, gestión adecuada de contraseñas, Control de cambios, políticas y estándares de seguridad, y con esta estrategia conjunta, si estaríamos en

camino de poder mitigar los riesgos que podrían presentarse en el caso de querer ofrecer acceso remoto para mis aplicaciones internas a la red.

Ahora bien, los controles lógicos implican a su vez tecnologías disponibles con el fin de lograr un acceso remoto seguro, entre estas tecnologías podemos mencionar las siguientes:

- ✚ VPN (Virtual private network)
 - IPSEC (IP seguro)
 - SSL (Secure Socket Layer)
- ✚ PKI (Public Key Infraestructura)
- ✚ Smart Card Technology
- ✚ NAC (Network Access Controler)
- ✚ LDAP, Radius protocols
- ✚ Protocolos 3DES, AES, MD5, SHA-1
- ✚ Firmas digitales

Quizás podríamos hacer nuestra lista aun mayor, pero lo que queremos es mostrar que estas tecnologías existentes hoy en día, de un cierto nivel de complejidad y costos asociados no despreciables, son facilitadores de proyectos de acceso remoto, pero sin estar integradas dentro de una estrategia conjunta de seguridad, podrían presentar vulnerabilidades explotables por un agente externo o interno a la entidad.

Podríamos concluir que toda decisión que conlleve a colocar la información o los recursos a usuarios externos debe pasar por un proceso de análisis de riesgos asociados, debe estar dentro de una estrategia unificada, contar con tecnologías que apoyen estos procesos con una gestión inteligente, deben incluir procedimientos y estándares, es decir, controles administrativos adecuados y por ultimo requiere del aseguramiento de todos los elementos que de manera directa e indirecta se relacionen con los servicios que se están tratando de

ofrecer. En otras palabras, todo servicio nuevo a implementar debe contar con una estrategia conjunta y unificada de seguridad.

AUTOR: EL ing Rodrigo Ferrer (rodrigo.ferrer@sisteseq.com) es egresado de la universidad de los Andes como ingeniero Eléctrico, en donde también ha realizado estudios de postgrado y especialización en telecomunicaciones y Gestión de sistemas de información. Se ha desempeñado laboralmente en empresas de redes y seguridad tales como: 3com, Extreme Networks, Sonicwall, Sisteseq, desempeñándose como Network Consultant para la región andina y como académico en varias universidades del país. Recibió en el 2006 la certificación CISSP (Certified Information System Security Profesional) del International Information Systems Security Certification Consortium (www.isc2.org), la certificación internacional más reconocida a nivel mundial en el área de seguridad de la información, seguridad física y seguridad en redes. También está en proceso de obtener la certificación CISA de ISACA y es LEAD AUDITOR 27001.

Como complemento a su formación tecnológica, ha realizado también realizado estudios de educación continuada en la Universidad de Cambridge en el Reino Unido y actualmente está finalizando la Maestría en Filosofía, en la Universidad Javeriana orientado al tema "filosofía de la ciencia y la tecnología".