En este artículo se analizan cuestiones clave relacionadas con la seguridad de las redes de empresa desde una perspectiva de actualidad: el reto que para los sistemas de información de las compañías supone la cada vez mayor apertura de los mismos como consecuencia de la generalización de Internet y del acceso remoto de los usuarios. Se abordará la seguridad desde un enfoque holístico, es decir, entendiendo la seguridad con un enfoque global, distribuido y completo

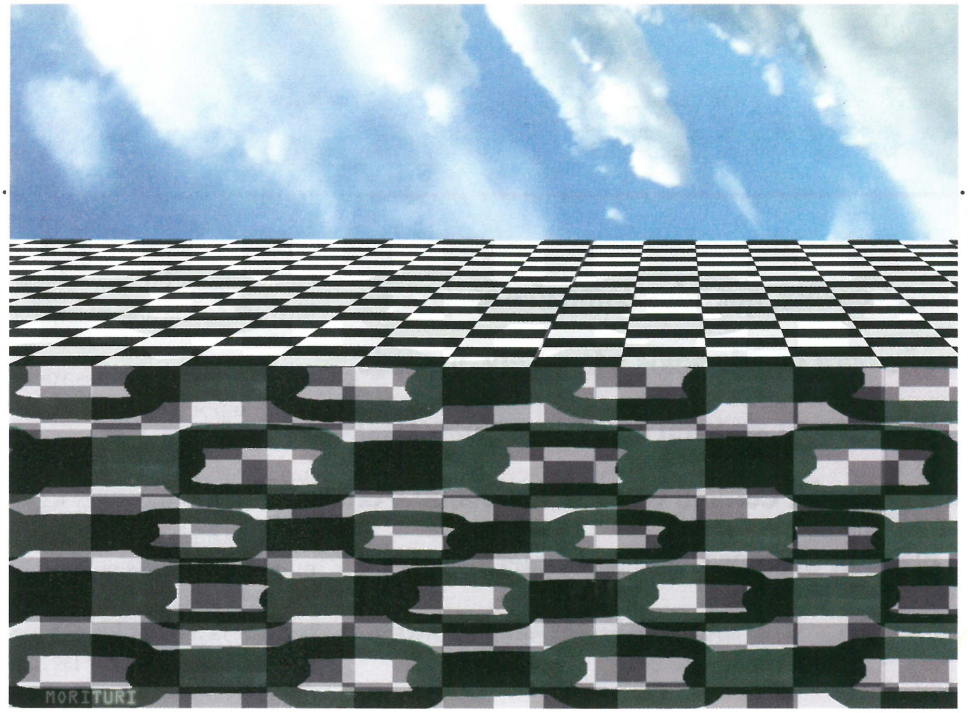
Seguridad en redes: un enfoque holístico

A la hora de abordar la seguridad en redes, lo primero que constatamos es que la realidad actual es radicalmente distinta a la de hace unos años. Aunque el objetivo último sigue siendo el mismo – minimizar el riesgo protegiendo los sistemas y la información crítica de las compañías de la perdida o uso indebidos – ni los peligros a los que los sistemas están expuestos ni las condiciones de entorno tienen mucho que ver con la situación actual.

Hasta hace no mucho los sistemas de información eran sistemas eminentemente **cerrados**. Por un lado, contar con una tecnología propietaria aseguraba en buena medida el aislamiento exterior. Por otro lado, las diferentes áreas departamentales de las compañías contaban con sistemas de información propios y a menudo aislados del resto de los sistemas de la compañía. Evidentemente, el principal problema de seguridad al que se enfrentaban estas compañías era la pérdida accidental de los datos por fallos de los sistemas, problema que se solventaba a través de sistemas de backup o sistemas redundantes.

Sin embargo, como se ha mencionado más arriba, la realidad de las compañías ha cambiado radicalmente, apareciendo nuevos retos de seguridad a los que es necesario enfrentarse. Estos retos vienen y vendrán en un futuro inmediato de:

- **Nuevos usuarios internos y externos:** Las demandas de acceso a los sistemas de información de las compañías están creciendo a pasos agigantados. Por un lado, los clientes quieren acceder a la información de la compañía, y lo hacen frecuentemente a través Internet. Por otra parte, cada vez es más frecuente que los trabajadores de las compañías se encuentren fuera de las oficinas centrales, donde la seguridad está garantizada: trabajadores desplazados, trabajadores que realizan su tarea en las dependencias del cliente, agentes comerciales... Todos ellos necesitan acceder a información crítica de la compañía y lo hacen a través de redes públicas como Internet.
- **Interconexión de áreas departamentales:** Hoy en día, dadas las crecientes exigencias en la atención al cliente, es impensable que los sistemas de información de cada departamento sean islotes autosuficientes y sin interconexión. El cliente demanda información y quiere tener un único interlocutor. El departamento comercial o de atención al cliente necesita acceder de forma directa a datos de dife-



• **Juan José Martínez Pagán**
Director Regional Sur Europa
Enterasys Networks

rentes áreas: comercial, personal, financiera, producción, etc. Por tanto, el añadido en seguridad que procedía del aislamiento desaparece.

- **Comercio electrónico:** Que la seguridad y el comercio electrónico son dos asuntos íntimamente relacionados es un hecho que nadie discute. Se ha hablado hasta la saciedad de que uno de los condicionantes fundamentales del despegue del comercio electrónico es la seguridad. Esto presenta además dos facetas: por un lado, hay que asegurar las transacciones entre cliente y proveedor. Por otro lado, comercio electrónico supone miles de usuarios entrando a nuestros servidores a la búsqueda de información. Nos encontramos de nuevo ante un nuevo reto de seguridad.
- **Multiplicación de usuarios y dispositivos:** Hasta la fecha el número de internautas ha sido relativamente pequeño. Esté número se va a incrementar exponencialmente con tecnologías como WAP y la futura telefonía móvil de banda ancha, sobre todo en países como España con una importante base instalada de usuarios. Hay que añadir la aparición de multitud de dispositivos diferentes que permitirán el acceso a Internet. Todo ello representa una amenaza para la seguridad.
- **Conectividad permanente:** Entrar en el mundo Internet supone empezar a jugar con sus propias reglas. Internet es conectividad permanente las 24 horas durante 365 días al año. No vale apagar los servidores cuando se cierra la oficina. En ese tiempo, alguien, desde la otra punta del globo puede comenzar sus ataques justo cuando la última luz del edificio se apaga.

UN ENFOQUE HOLÍSTICO

Nuevos retos exigen nuevos enfoques. Hasta ahora, la seguridad de las redes se ha venido gestionando en mi opinión de una manera tradicional. Se han utilizado los mecanismos y sistemas que se han utilizado tradicionalmente en los sistemas cerrados, implantando soluciones de seguridad concretas a los nuevos problemas que van surgiendo.
En mi opinión, el nuevo paradigma requiere un enfoque radicalmente diferente y de visión global, que vaya más allá de soluciones "locales". Este nuevo planteamiento lo podríamos denominar "holístico"
Se denomina holístico – de origen griego- a aquel planteamiento que considera que una realidad compleja es algo más que la mera suma de todos sus elementos, y que constituye un sistema global regido por leyes propias.
En mi opinión, la seguridad de una red debe entenderse de manera holística: requiere de un enfoque global, distribuido y completo, es decir ha de ser:

- **Global**: La seguridad debe entenderse como una arquitectura. Debe abarcar toda la infraestructura de red e integrar e un mismo sistema los diferentes elementos que integran los diferentes sistemas de seguridad: firewall, VPN, IDS, etc. Es asimismo imprescindible que todo el sistema esté basado en estándares, que aseguran la total integración.
- **Distribuida:** "Una cadena siempre se rompe por el eslabón más débil", dice un viejo proverbio. Los sistemas de seguridad no sólo deben proteger y residir en el núcleo de nuestro sistema de información. El nuevo paradigma apuntado anteriormente exige que todas las ramificaciones de la red, tanto físicas como virtuales, locales y remotas, estén totalmente protegidas.
- **Completa:** La seguridad debe abarcar todo el camino que recorre un usuario desde que accede a nuestra red por el punto de acceso hasta que alcanza su objetivo. El objetivo es seguir la pista a ese usuario en todo momento, asegurándonos de que es auténtico y de que está autorizado. Sólo así se puede tener el control en las máximas condiciones de seguridad.

La infraestructura de seguridad desde un punto de vista holístico debe ser una capa transversal que abarque todos los sistemas de la red: gestión, infraestructura de routing y switching, redes privadas virtuales, accesos "wireless".
En conclusión, creo que este enfoque es el más adecuado en lo que respecta a seguridad, habida cuenta de los retos a los que se enfrentan las compañías hoy en día en este ámbito, máxime si se tiene en cuenta que día a día aparecen nuevos desafíos para las redes corporativas. El desafío fundamental es conseguir que nuestro sistema de información satisfaga cuatro elementos clave: velocidad, flexibilidad, fiabilidad y **seguridad,** todo ello al servicio de los clientes externos y externos las 24 horas al día durante 365 días al año. Adoptar un enfoque holístico en seguridad nos permite cumplir con todos los requisitos.