

AMENAZAS INTERNAS Y NORMATIVAS DE PRIVACIDAD

Nuevos retos para la seguridad de red



Francisco García

Director técnico sur EMEA. Enterasys

La frecuencia con la que se producen incidentes de seguridad se ha incrementado rápidamente en los últimos años, con un crecimiento exponencial desde 1998. Estos incidentes están en gran parte causados por los nuevos virus y gusanos, que se propagan utilizando las propias redes a velocidades vertiginosas

Por poner un ejemplo, un virus actual, sofisticado, y que se aprovecha de las capacidades de las redes para infectar las máquinas, es capaz de replicarse a una velocidad muy superior a los de hace sólo un año. La capacidad de infección inicial del virus "Slamer" es de 420 host en una hora, frente a los 1,8 host que alcanzaban virus como "Code Red", y es capaz de duplicar el número de máquinas infectadas en sólo 8 segundos. Las pérdidas causadas a empresas en todo el mundo por virus y gusanos se cifran en 180.000 millones de dólares.

Esto ha traído como consecuencia fundamental que la mayor parte de las iniciativas de seguridad puestas en marcha por las empresas hayan estado destinadas a combatir las amenazas externas. Sin embargo, las organizaciones de hoy día se enfrentan a dos nuevos retos: protegerse de las amenazas internas y cumplir con los requisitos de confidencialidad de datos que incluyen la mayoría de los países en sus ordenamientos

AMENAZAS INTERNAS

Las organizaciones de la actualidad tienen poco que ver con las empresas de hace unos años. El perfil de empleado con 20 años de trayectoria profesional dentro de la compañía prácticamente ha desaparecido. La realidad empresarial actual hace que hoy día tengan acceso a los sistemas de información de las compañías un abanico de usuarios mucho más diverso: empleados, socios, clientes, proveedores, trabajadores de terceras compañías en outsourcing, etc.

Cuando la empresa interactúa con cualquiera de estos nuevos usuarios, es casi obligado que les dote de algún tipo de conectividad, para que puedan realizar sus tareas. Este nuevo conglomerado de usuarios representa una amenaza potencial para los sistemas de la empresa, incluso en el caso de que ninguno de ellos realice acciones malintencionadas. Simplemente el acceso o utilización inadecuada a determinados recursos puede causar un perjuicio considerable.

Por tanto es preciso contar con los mecanismos que permitan, de una ma-

nera automatizada y dinámica aislar a los diferentes grupos de usuarios, dotándoles de capacidades de acceso y utilización de los recursos de red en función de su relación con la compañía. Se trata de evitar que puedan acceder a determinados recursos de la empresa, pero que tengan acceso a los suficientes como para poder desarrollar con éxito su trabajo.

REGULACIÓN EN MATERIA DE DATOS SENSIBLES

La regulación en materia de protección de datos de ciudadanos es cada vez más estricta en la mayoría de los países de nuestro entorno. Cada vez más compañías, sobre todo de determinados sectores (Administración Pública, Sanidad, Educación, Seguridad, etc.)

Las empresas se están concienciando de los problemas legales que puede ocasionarles una filtración o pérdida de datos personales de clientes o ciudadanos, en un momento en que la sociedad está especialmente sensibilizada con este tema.

En este punto volvemos a lo anterior. Es una falacia pensar que "los malos" están fuera del perímetro de nuestros sistemas de información y "los buenos" dentro. Estudios realizados en Universidades demuestran que un alto porcentaje de las amenazas de seguridad provenían de profesores, alumnos y empleados poco sospechosos. Se trata de proteger la información sensible no sólo de los ataques de "hackers", sino también del uso inadecuado por parte de usuarios internos a la organización.

