



Seguridad en redes IP

Javier Cuenca

*Consultor Senior del Área de Ingeniería de Sistemas
de Nextel Engineering*

En este preciso momento existen más de 1.100 millones de usuarios conectados a Internet, según la IWS. Hipotéticamente, si consideramos que el diez por ciento de esos usuarios puede plantearse, en un momento dado, el ataque a un sistema, ya sea para obtener un beneficio económico o una información privilegiada o, simplemente por diversión, y que de esos ciento once millones el diez por ciento (unos once millones de usuarios) tiene conocimientos para poder hacerlo, llegaremos a la conclusión de que existe un peligro latente para nuestras redes.

Además, si a todo eso le agregamos los problemas propios del *hardware*, *software* y usuarios, lo que tenemos es un pequeño problema que debe solucionarse rápidamente de la forma más ágil y eficaz posible.

Confidencialidad e integridad

Para paliar esa carencia lo primero que debemos tener claro es que la seguridad absoluta no existe. Por tanto, lo que hemos de encontrar es un equilibrio entre la protección de nuestros servicios ofrecidos en la red y la facilidad con la que los usuarios acceden a esos servicios, tratando de mantener, en la medida de lo posible la confidencialidad, disponibilidad e integridad de la información que se ofrece.

Entonces, ¿qué hacemos? En primer lugar, es importante tener muy claro qué es lo que

nos interesa proteger. A continuación, lo propio sería preguntarnos: ¿de qué debemos preservarlo? Para empezar, se debería prevenir el sistema contra posibles interrupciones. Una vez hecho eso, se instalarían aplicaciones que imposibilitaran la interceptación, destrucción, fabricación o modificación de información contenida en nuestra red.

Después de haber definido qué y cómo debemos protegernos es muy importante tener más o menos claro el origen de los ataques y el perfil de quién los lleva a cabo. Normalmente, se corresponden con empleados, ex empleados, intrusos remunerados, curiosos, terroristas de la información, usuarios avezados o con graves errores de conocimiento, así como *software* malintencionado, bombas lógicas, virus, etcétera. Por esta razón, se debe trabajar en un conjunto de documentos que definan el plan de recuperación ante desastres. Para ello, se debe comenzar realizando un análisis de riesgos y amenazas que abarque todos los puntos de nuestra red. Obviamente, cuanto más profundo sea dicho análisis mejor sabremos actuar ante una incidencia.

Ese diagnóstico sobre los posibles riesgos y amenazas permitirá definir una política de seguridad corporativa, que tendrá como finalidad la prevención de la red durante su funcionamiento diario, la detección de incidencias en el momento en que se produz-

can y la recuperación de la red en el mínimo tiempo posible y con el menor impacto para los usuarios.



El análisis sobre la vulnerabilidad de la compañía dependerá de cuestiones como el grado de publicidad o el tipo de negocio

El análisis sobre la vulnerabilidad de la compañía dependerá en gran medida de cuestiones como el grado de publicidad de la compañía, el negocio de ésta y su exposición a riesgos internos y externos. Lógicamente, cuanto más conocida sea la compañía, mayor será el número proporcional de ataques potenciales.

Amenazas y sus tipos

Como ya hemos comentado anteriormente, una amenaza consiste en cualquier circunstancia que, de forma real o hipotética, pueda provocar un daño a nuestra compañía mediante la exposición, modificación o destrucción de alguno de sus datos o servicios. Sin embargo, podemos concretar más diferenciando las amenazas en función del tipo de daños que puedan ocasionar:

1. Fallos de componentes, tanto *hardware* como *software*.
2. Exposición de la información o los datos de nuestra compañía.
3. Utilización de la información o los datos para usos no previstos.
4. Borrado o modificación de la información o datos, pérdidas de confidencialidad, etc.

Servicios que comprometen la red

El acceso remoto de usuarios, el correo electrónico, las páginas web y, en teoría, todos aquellos servicios en los que están involucrados usuarios e información de la compañía, más o menos confidencial, pueden poner en peligro la seguridad de la red. Aunque también debe prestarse una atención especial a cuestiones aparentemente sin importancia

como las contraseñas fáciles de recordar (en ocasiones se da el caso contrario, las contraseñas son demasiado difíciles y se apuntan en lugares de fácil acceso para amigos de lo ajeno), las cuentas de usuario inactivas, los servicios mal configurados, las soluciones activas poco o nada necesarias para la compañía, los puestos de cliente en portátiles sin seguridad y con información privilegiada, las versiones antiguas de sistemas operativos, los módems repartidos por la empresa sin control o las políticas de copias de seguridad inexistentes o mal diseñadas.

¿Cómo saber que hay un problema?

Lo ideal es que tengamos controlado el problema incluso antes de que ocurra, trabajando para ello de forma pro-activa. Aunque conseguir esto es complicado, en un entorno de red auditado y monitorizado por un profesional, y con una configuración de sistema que avise del hallazgo de discrepancias (gracias a procedimientos de seguridad coherentes y actualizados), se podrá comprobar, mediante la combinatoria de contadores y auditoría, si la tendencia de nuestra red va hacia una parada de servicio, hacia un servicio deficiente o hacia un servicio degradado. A partir de ahí, pistas como servidores que se paran sin motivo, discordancias en cuentas, intentos de escritura en archivos del sistema, accesos a horas intempestivas, etcétera, nos indicarán la posibilidad de que exista alguien intentando acceder a nuestro sistema.

Conclusiones

Para contar con una red segura es necesario disponer de un amplio abanico de recursos y servicios capaces de proteger la información en todo su ciclo de vida. Sin embargo, no debemos caer en el error de olvidar la importancia de contar con una buena política empresarial en materia de seguridad y con un buen plan de recuperación, ya que sin esto seguiremos siendo vulnerables y no estaremos en disposición de recuperar la información original, ni de volver a la normalidad sin sufrir las consecuencias.