

# Principales preocupaciones administradores de redes en 2008

**AL IGUAL QUE EN AÑOS ANTERIORES, EN 2008 LOS ADMINISTRADORES DE RED Y SISTEMAS TENDRÁN QUE ENCARAR DESAFÍOS QUE PONDRÁN A PRUEBA SUS HABILIDADES PARA PROTEGER ADECUADAMENTE LAS REDES CORPORATIVAS.**

**Z**a experiencia muestra que el mantenimiento y la mejora de la seguridad nunca es fácil: hackers, creadores de software malicioso, spammers, amenazas internas y otros, la mayoría de ellas impredecibles, forman parte de las causas para que estos profesionales de la seguridad pasen muchas noches en vela.

Varias predicciones sobre amenazas para el 2008 ya han saltado a los titulares. Algunos mencionan VOIP y virtualización, otros la evolución del malware y de los accesorios de Facebook que se utilizarán para distribuir malware. Aún así, los hechos y las cifras sobre los desafíos en materia de seguridad que se deberán encarar durante el 2008, indican que los mayores peligros no vendrán de la tecnología en sí, tratándose al fin y al cabo de un elemento neutral que puede ser utilizado, tanto para el bien, como para el mal. La mayor amenaza durante el 2008 seguirá siendo, de este modo, la misma que ha estado amenazando a las empresas durante los últimos 200.000 años – ¡el propio Ser Humano! Los seres humanos, sus debilidades, falacias y curiosidad seguirán siendo explotados, de este modo, para causar auténticos destrozos en las organizaciones.

## **LA CONFIANZA EXCESIVA**

La historia nos muestra que tendemos a confiar demasiado en los reclamos de los fabricantes de sistemas operativos y aplicaciones empresariales. Los nuevos sistemas siempre se venden como más seguros y más infalibles que sus predecesores, y aunque eso sea indudablemente cierto, uno debe recordar que al presentar cada nuevo sistema operativo y aplicación empresarial a través de los años, los fabricantes han hecho la misma afirmación, una y otra vez, año tras año. Esto, sin embargo, nunca ha disuadido a los hackers y otros individuos maliciosos de investigar y perpetrar ataques contra los sistemas

operativos más innovadores. Un claro ejemplo de ello es Microsoft Windows Vista, que para finales de 2007 esperaba alcanzar una cuota de mercado del 10%, con un ratio de adopción proyectado del 30% para finales de 2008. Microsoft Windows Vista no sólo equivale a un nuevo sistema operativo, sino también a una nueva experiencia de usuario. Aunque este sistema

**Cuando se trata de seguridad de red, la ignorancia no es excusa. En 2008, el desconocimiento de principios básicos de la seguridad y de la evolución que está sufriendo el malware, spyware y otros, contribuirán de manera muy significativa al colapso de la seguridad de red.**

sea mucho más seguro que sus predecesores, sus usuarios siguen siendo los mismos y, por lo tanto, siguen ofreciendo la ruta de menor resistencia para aprovecharse de los entornos de red más habituales. Mediante ingeniería social, barreras para la seguridad como el nuevo control de acceso de usuario pueden ser fácilmente burladas, engañando a los usuarios para que los mismos instalen software no seguro o contaminado con malware.

## **LA FE CIEGA**

La confianza debe ganarse y no otorgarse automáticamente. Los peligros para el negocio no provienen únicamente desde el exterior de la empresa. La historia más reciente muestra que los ataques internos cuestan a los negocios tanto o más, que los ataques originados desde fuera. Los autores internos de estos ataques aventajan a sus competidores desde el exterior, ya que cuentan con un conocimiento íntimo de la red corporativa y de su funcionamiento interno.

En 2008, el continuo incremento en el uso de dispositivos portátiles de almacenamiento y comunicación (como iPods, USBs, placas WiFi USB, etc.) facilitarán aún más el robo de información, las bombas lógicas y otras formas de sabotaje que pueden arrojar de nuevo a un negocio a la Edad de Piedra. Una vez más, y aunque sería fácil culpar a dichos dispositivos, no es en ellos donde radica el fallo. Recordemos de nuevo que la tecnología es un elemento neutral y que el fallo, en estos casos, no está en el dispositivo en sí, sino en el uso que se le da. Prohibirlos para evitar el problema simplemente no funcionará, dado que no se puede confiar en el cumplimiento voluntario de una prohibición de este tipo. La supervisión necesaria, por otro lado, resultaría demasiado laboriosa, ya que estos dispositivos pueden ocultarse fácilmente y sólo conseguiríamos crear malestar en la organización.

#### LA FALTA DE CONOCIMIENTO

Cuando se trata de seguridad de red, la ignorancia no es excusa. En 2008, el desconocimiento de principios básicos de la seguridad y de la evolución que está sufriendo el malware, spyware y otros, contribuirán de manera muy significativa al colapso de la seguridad de red. Lo más habitual es que esto sea debido a falta de tiempo o recursos para investigar acerca de los principios y tendencias en este tipo de ataques. Se trata de un problema que obligará a la compañía a adoptar un acercamiento "apagafuegos": reaccionando ante las incidencias una vez que la red haya sufrido el ataque.

Se trata, de nuevo, de un problema de carácter humano. El software malicioso no evoluciona por sí solo y de forma aislada. La razón por la que el malware adopte continuamente nuevas formas y se extienda cada vez más es principalmente

la codicia. Los hackers y demás individuos malintencionados hoy ejecutan ataques cuyo fin último no suele ser la destrucción, sino las ganancias financieras.

Los abusos con un determinado target que intentan aprovecharse de la curiosidad natural de las personas para hacerles pulsar sobre un enlace contaminado se volverán más y más comunes. Esto les hace más peligrosos que nunca, haciendo





incluso más crítica la falta de conocimiento. Limitar la curiosidad humana mediante una prohibición total de acceso a recursos será también contraproducente ya que generará malestar y aburrimiento, que a su vez golpean la productividad.

**LA INGENUIDAD**

Ser ingenuo no sólo convierte a la persona en blanco de las bromas, sino que además

le expone a múltiples amenazas relacionadas con la seguridad de red. En 2008, los e-mails de spam dirigidos continuarán evolucionando hacia nuevas y originales tentativas para burlar las defensas de la red, utilizando la ingeniería social. Estos se extenderán más allá del e-mail e intentarán, por ejemplo, comprometer las infraestructuras de VOIP mediante ataques de denegación de servicio, vulnerabilidades SIP y ataques Spiti (Spam Over Internet Technology). En 2008, también se espera un incremento en el número de

ataques dirigidos a individuos o negocios específicos, y es muy posible que los autores de dichos ataques utilicen la ingeniería social para asegurarse el acceso a la información confidencial que les permita acceder a los sistemas.

Al igual que en el caso del malware, la ingeniería social

**La confianza debe ganarse y no otorgarse de forma automática. Los peligros para el negocio no provienen únicamente desde el exterior de la empresa. La historia reciente nos ha demostrado que los ataques internos cuestan al negocio tanto o más que los originados desde fuera.**

intenta aprovecharse de la ingenuidad humana para obtener ganancias financieras. Nadie llamará a nadie pidiendo contraseñas. Se aplicarán, de este modo, métodos más sutiles como por ejemplo los ataques dirigidos en redes sociales (myspace, facebook, etc.) donde los usuarios son engañados para intercambiar información personal por bienes virtuales, permitiendo a los hackers y otros individuos malintencionados a obtener un acceso no autorizado a redes.

**A MODO DE CONCLUSIÓN**

En 2008, los administradores de red y los encargados de la seguridad tendrán que disfrazarse más que nunca y emplear toda clase de defensas contra ataques dirigidos a debilidades de las personas, como: el exceso de confianza, la fe ciega, la falta de conocimiento y la ingenuidad. Todas estas "debilidades", por otro lado, se convertirán en factores decisivos para mostrar hasta qué punto será exitosa la seguridad de red. Más que nunca, la seguridad de red se convertirá en una cuestión de administrar adecuadamente los riesgos que personas suponen para el negocio. Aún y cuando los riesgos que provienen de las personas sigan siendo los mismos que antes, durante el presente año se observará un cambio en la motivación de los ataques, que se volverán mucho más peligrosos.

En 2008, de este modo, los administradores de sistemas tendrán que encontrar la forma de garantizar el equilibrio entre frenar los peligros para la red provenientes de la natural curiosidad humana, evitando a la vez los métodos de la Inquisición Medieval.

**DEFENSAS**

Existen múltiples maneras para que los administradores puedan defender las infraestructuras corporativas de posibles amenazas, considerando como imprescindibles:

- Monitorizar la actividad de los usuarios 24 x 7 x 365
- Controlar el acceso a los recursos de la red
- Salvaguardar toda la información empresarial
- Copiar todas las comunicaciones desde, hacia y dentro de la empresa
- Establecer barreras tecnológicas que permitan el uso de dispositivos de acuerdo a una directiva clara y definida.
- Formar adecuadamente a los usuarios de recursos de la red, tanto en seguridad de red, como en las políticas de uso y divulgación de información.



**JASON MICALLEF** ES RESPONSABLE DE INVESTIGACIÓN TÉCNICA DE GFI