

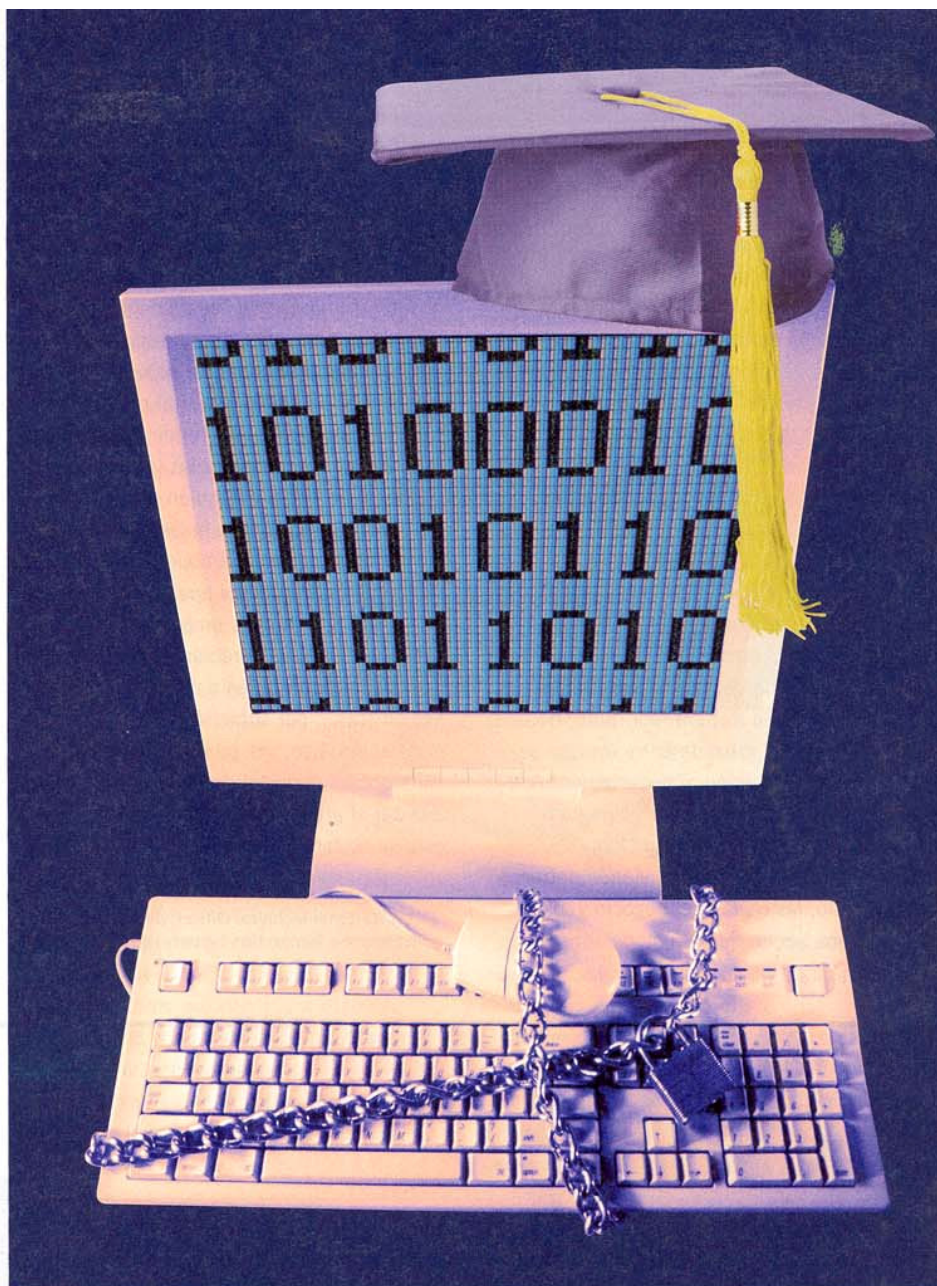
Sin embargo, las pymes son igualmente conscientes de que no cuentan con el presupuesto suficiente para gastar miles de euros en algo en lo que ven poco retorno de la inversión a corto plazo. La lucha de voluntades entre el administrador de la red y la dirección es más evidente en pymes, donde más del 50% reconoce tener problemas a la hora de convencer al equipo directivo para invertir en determinadas soluciones de seguridad, según recientes estudios de GFI llevados a cabo en EE.UU.

Seguridad en torno a los usuarios

Los usuarios informáticos pueden considerarse como la menos predecible y controlada vulnerabilidad de seguridad. En la mayoría de casos, una falta de información y un desconocimiento de los principios y procedimientos básicos de seguridad son las principales causas de los agujeros de seguridad en lugar de la actividad maliciosa —aunque esto último no se puede ignorar—. Sin embargo, el resultado final es habitualmente el mismo: se pierde información inestimable, la empresa pierde credibilidad, etc.

Según una encuesta realizada a 455 ejecutivos de TI de PYMES en EE.UU., el 48% afirmó que el conocimiento de asuntos de seguridad por parte de los empleados —el eslabón más débil ante una vulnerabilidad— fue un factor clave

Aunque muchas pymes no sean conscientes de ello, la pérdida de información sensible puede tener un impacto devastador en el balance de una empresa



para conseguir una mejor seguridad global de los sistemas informáticos de la empresa.

Y es que, aunque no lo parezca, es realmente fácil que se produzca una vulneración de la seguridad de las redes de información de una compañía. Es habitual la pérdida de grandes cantidades de información porque los empleados ponen sus contraseñas en adhesivos sobre sus monitores, olvidan portátiles o dispositivos de mano en aeropuertos, gimnasios y restaurantes o en sus coches. También mantienen sus equipos desbloqueados o encendidos durante almuerzos, dejan sin atención sticks USB con información empresarial sensible o navegan por Internet desde sus casas mientras están conectados a sus redes empresariales. Por poner un ejemplo de las repercusiones que estas

fugas de información pueden tener, cabe citar el caso de un ciudadano norteamericano que tropezó con un *stick* de memoria en una estación de servicio en Azle, Texas, que contenía información sobre el Joint Strike Fighter, el más caro programa armamentístico de los EE.UU. Aunque muchas pymes no sean conscientes de ello, la pérdida de información sensible puede tener un impacto devastador en el balance de una empresa.

Subestimando las amenazas

Según el ya citado estudio llevado a cabo por GFI entre diferentes pymes de EE.UU., se muestra que 4 de cada 10 pymes aseguraron que sus redes no eran lo suficientemente seguras, siendo los virus la principal amenaza de seguridad. Cuando se les preguntó cuáles eran sus

La educación de los empleados, principal reto para la seguridad de las pymes

principales preocupaciones diarias, el 71% de los encuestados citó las caídas de sistema y la dedicación a cuestiones de seguridad, mientras que el 51% apuntó al soporte al usuario como su preocupación diaria.

Queda claro que las empresas están subestimando la amenaza.

Desafortunadamente, incluso enfrentados con dichas pruebas, muchos negocios todavía creen que no les ocurrirá a ellos, siendo esto un grave error. Aun así, la mayoría de directivos está familiarizado con los productos de seguridad tradicionales, particularmente anti-virus, anti-spam y cortafuegos. Los administradores de TI encuentran pocos problemas a la hora de adquirir estos productos, sin embargo convencer a la Dirección de gastar en gestión de vulnerabilidad, administración de



La mayoría de pequeñas y medianas empresas reconocerá el hecho de que la seguridad en TI es un tema importante, y que el riesgo de brechas de seguridad, fugas o pérdidas de información nunca ha sido mayor. Junto con el número de vías en que la información puede ser almacenada y transferida, aumenta en la misma proporción las vulnerabilidades de las redes amenazando seriamente la solidez de los negocios y la privacidad de sus clientes.

Convencer a la Dirección de gastar en gestión de vulnerabilidad, administración de registros de sucesos y soluciones de administración y archivado de correo es todo un problema



registros de sucesos y soluciones de administración y archivado de correo es todo un problema. Y esto bien podría explicar por qué el 25% siente que la dirección necesita más conocimiento de las amenazas de seguridad que encaran las empresas hoy en día.

Soluciones al problema

Las pymes necesitan tomar medidas preventivas de seguridad para evitar que ocurran fugas mediante la pertinente información a sus empleados en materias de seguridad y barreras tecnológicas que impongan la directiva de la empresa. Es necesario hacer un mejor uso de las herramientas que están disponibles para los equipos informáticos y comenzar a ver la seguridad como una inversión en lugar de como un gasto. La clave radica en dirigirse a compañías de software que ofrecen funcionalidad empresarial y software de calidad a un precio que se pueden permitir las pequeñas y medianas empresas. Es importante que los administradores de TI y los gestores de las áreas de negocio empiecen a hablar el mismo lenguaje y entiendan lo que concierne a cada uno. Ya que el factor humano es el eslabón más débil a la hora de proteger la red informática de una empresa, se pueden seguir estos 10 pasos para proteger las redes de vulnerabilidades humanas: Comenzar con la dirección. Cuando la dirección comprenda y actúe en

beneficio de la seguridad, se habrá ganado media batalla. Implantar una directiva de seguridad claramente definida y sin complicaciones. Respaldarla con una comunicación clara. Educar a los empleados para tener cuidado de no dejar en marcha sus dispositivos móviles. Hacerles comprender que es un riesgo. Instruir a todo el personal en los conceptos básicos de la seguridad

La clave radica en dirigirse a compañías de software que ofrecen funcionalidad empresarial y software de calidad a un precio que se pueden permitir las pequeñas y medianas empresas

informática, como buenas prácticas en el uso de contraseñas, etc. La educación es clave para la seguridad de su red. Introducir medidas de seguridad no estándar como escáneres biométricos para las principales áreas de seguridad, habitualmente es más barato que un incidente de robo de información. Restringir estrictamente el acceso remoto a la red a quien lo necesite. Esto también se puede aplicar al acceso a Internet mediante el enrutador de la empresa. Monitorizar el uso de los empleados de los recursos de sus equipos. Establecer el control sobre su red empresarial. Limitar los cambios de los

usuarios a las opciones del equipo y de las aplicaciones instaladas. Limitar la navegación, mensajería instantánea, uso de aplicaciones *peer-to-peer* y que se compartan archivos. Restringir el uso de dispositivos portátiles de almacenamiento. Utilizar sólo soluciones que le permitan el acceso lectura/escritura o el bloqueo del acceso a aquellos que no necesiten utilizar estos dispositivos. Implantar una estricta directiva de contraseñas. Cambiar regularmente contraseñas/códigos de acceso para limitar los daños causados por fugas debidas a ingeniería social.

Las vulnerabilidades en materia de seguridad y el robo de información pueden ocurrir en cualquier momento. Sin embargo, hay formas eficaces de limitar el riesgo de que alguien desde algún lugar esté esperando pacientemente para infringir serios daños en la red de la compañía y robar información. Con la adecuada política de seguridad, las PYMES pueden proteger satisfactoriamente sus negocios de daños financieros, legales y salvaguardar su reputación.

www.gfi.com.

Autor: Andre Muscat, director de ingeniería de GFI Software