

Los 10 principales errores de seguridad de las pyme

LA MAYOR AMENAZA A LA QUE DEBERÁN ENFRENTARSE LAS EMPRESAS EN LOS PRÓXIMOS AÑOS SERÁ LA MISMA QUE HA AZOTADO AL MUNDO EN LOS ÚLTIMOS 200.000 AÑOS: EL SER HUMANO. LAS DEBILIDADES, INCONGRUENCIAS Y CURIOSIDAD DE LAS PERSONAS SERÁN EXPLOTADAS PARA CAUSAR ESTRAGOS EN LAS ORGANIZACIONES.

Siempre que hay una brecha de seguridad o que algo va mal en la red informática de una empresa, suele ser por culpa de los usuarios finales. Los empleados a pesar de recibir extensas recomendaciones, docenas de e-mails y advertencias verbales, continúan ignorando las medidas de seguridad más básicas, como no dejar sus claves anotadas en un *post-it* pegado a su PC.

Sin embargo, aunque en el 99% de las ocasiones, es este el caso, hay veces en las que el dedo acusador debe señalar hacia la dirección menos esperada: el departamento de administración de TI.

Así es, incluso los administradores informáticos pueden cometer errores y lo hacen, especialmente en las pyme. A diferencia de los usuarios finales que normalmente ocasionan problemas por no desenvolverse con soltura en el mundo TI o por no comprender la lógica subyacente a la seguridad informática, se espera que los administradores de TI sean infalibles en materia de tecnología.

Las personas son el eslabón más débil en materia de seguridad y por ello, los administradores deben combatir todo tipo de ataques dirigidos a la naturaleza humana.

Desafortunadamente, con Internet y el agitado y exigente mundo tecnológico en el que vivimos, los administradores informáticos en las pyme se ven forzados a hacer mucho más que sentarse a monitorizar la red informática de la empresa. De hecho, son responsables de casi cada equipo de hardware en la compañía, incluso de la cafetera eléctrica. Son en realidad los "manitas" del edificio y, por si esto no fuera suficiente, también tienen que lidiar con los problemas de los usuarios finales, como la falta de conexión a Internet o cables mal conectados.

Demasiada carga de trabajo, poco tiempo, la presión de ajustarse a fechas tope, y mantener contentos a los superiores, lleva a los administradores informáticos a cometer errores de diagnóstico que pueden ser muy graves en algunas ocasiones. Para evitarlos, a continuación se detallan los diez principales errores o descuidos de los administradores de red:

1 Conectar sistemas a Internet antes de protegerlos. Este es un error clásico. Los ordenadores no están diseñados para conectarse a Internet nada más salir de la caja de embalaje. Antes de adquirir para el puesto de trabajo una línea de teléfono, un cable Ethernet o una tarjeta inalámbrica, es recomendable instalar al menos una solución de protección contra virus y detección de spyware, así como un programa para prevenir la instalación de software malicioso.

2 Conectar a Internet sistemas de prueba con cuentas y contraseñas por defecto. Esto es un sueño para un hacker. Dejar las claves y cuentas por defecto facilita enormemente a un hacker el acceso a la red informática. Solución: cambiar las contraseñas y borrar o renombrar las cuentas por defecto inmediatamente. También es conveniente asegurarse de que los empleados no tienen derechos de administrador en sus equipos, ya que no necesitan ese nivel de control sobre su ordenador.

3 No actualizar los sistemas. Existen multitud de agujeros de seguridad en los sistemas operativos y ningún software es perfecto. Una vez que se encuentra una vulnerabilidad, ésta se explota en muy poco tiempo, por

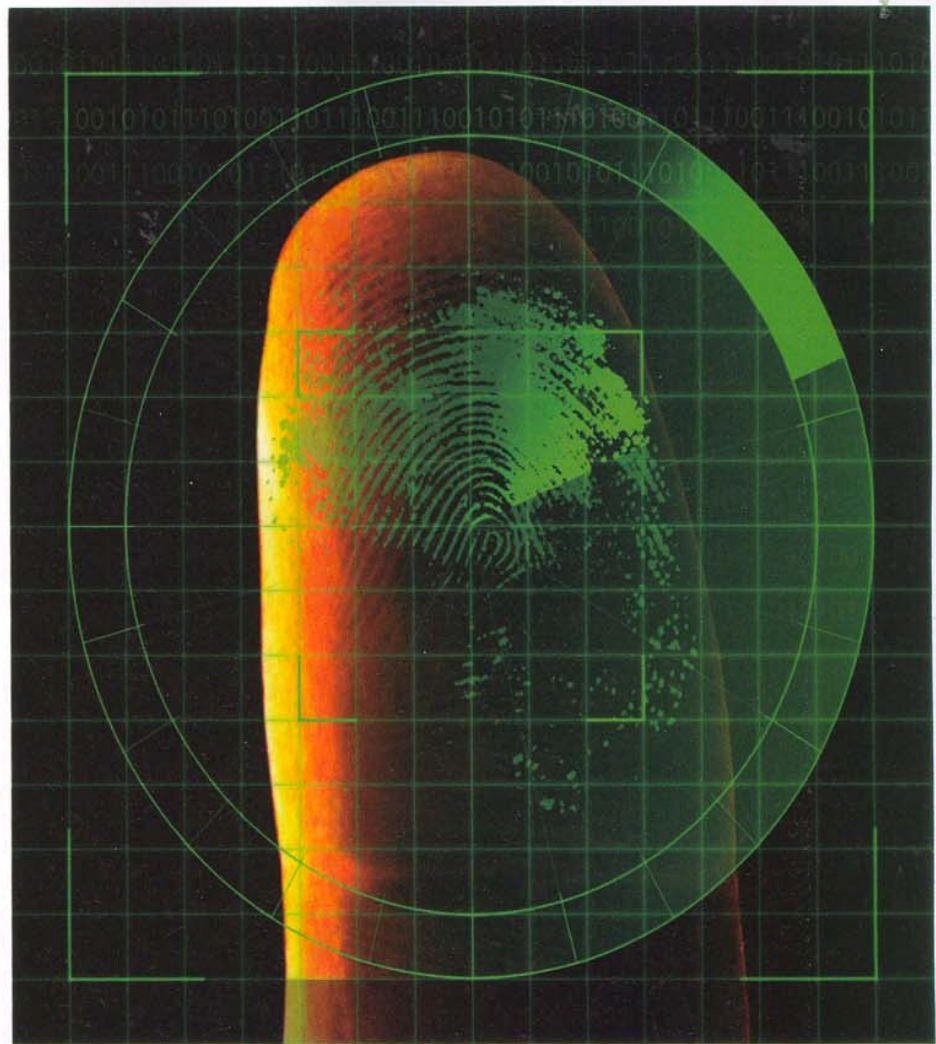
lo que es conveniente instalar parches de seguridad lo antes posible, incluso si se tarda en revisarlos en un entorno de prueba antes de su actualización.

4 Falta de una adecuada autenticación de los usuarios que solicitan servicios técnicos por teléfono. Facilitar a los usuarios contraseñas por teléfono o cambiárselas en respuesta a una solicitud telefónica o personal cuando el usuario no se ha identificado puede ser la mejor manera de reducir los trámites de las solicitudes de soporte impresas, pero facilita enormemente la labor de los hackers involucrados en tareas de ingeniería social. Lo mejor es reforzar la adecuada autenticación, incluso cuando la voz del interlocutor resulta familiar.

5 No mantener ni probar las copias de seguridad. La pereza es una de las mayores amenazas de seguridad. Sin embargo, la creación de copias de seguridad adecuadas es mucho más fácil que recopilar los datos desde cero. Por ello, es conveniente realizar a menudo copias de seguridad y mantenerlas alejadas incluso fuera de las instalaciones de la compañía (no en la caja fuerte del jefe).

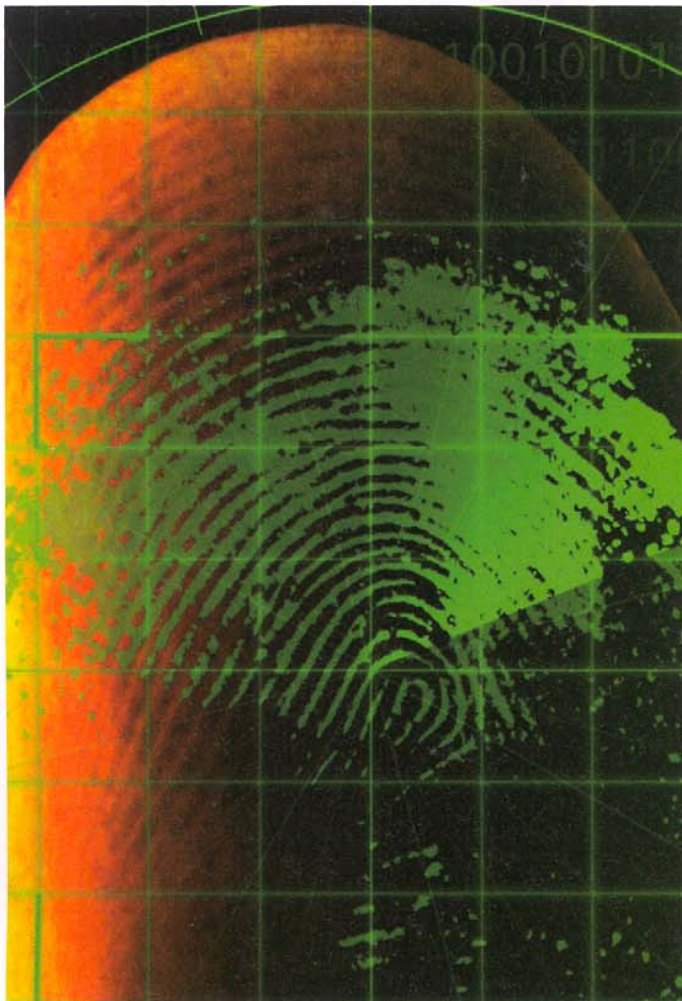
6 No confirmar que el plan de recuperación ante desastres realmente funciona. Una vez que se tienen las copias de seguridad, hay que preguntarse si funcionan, si se ha verificado que son buenas y si se tiene un plan de recuperación ante desastres. Si las tres respuestas son negativas nos encontramos ante un problema.

7 No implantar o actualizar programas de detección de virus. ¿Qué sentido tiene tener soluciones anti-virus y anti-spyware si no se actualizan? Las soluciones actualizadas aseguran que las últimas



modalidades de software malicioso serán detectadas inmediatamente, por lo que resulta altamente recomendable contar con una solución anti-virus permanente en cada equipo.

8 No formar a los usuarios en materia de seguridad. Los usuarios necesitan saber exactamente cuáles son las amenazas a las que deben enfrentarse. Los usuarios informáticos no formados en temas de seguridad, son aquellos que suelen ser víctimas de virus, spyware y ataques de phishing, diseñados para corromper sistemas o filtrar información personal a terceros sin el consentimiento del usuario. No hay que dar por hecho los conocimientos de los usuarios, ni confiar demasiado en ellos. Si se cuenta con políticas de seguridad dirigidas a los usuarios finales es conveniente asegurarse de que todos los empleados conocen su existencia y las cumplen.



9 **Tratar de hacerlo todo uno mismo.** Las grandes compañías cuentan con departamentos de informática considerables, pero los administradores de las PYMEs muchas veces se encuentran solos por lo que deberían pedir consejo y ayuda si se topan con dificultades a la hora de instalar la red informática. La ayuda externa, a pesar de ser costosa en ocasiones, asegura que el trabajo se hace bien a la primera.

10 **Fallos a la hora de reconocer las amenazas internas.** Demasiada confianza puede aniquilar la red informática de una empresa. Los empleados, sobre todo los descontentos, pueden causar enormes problemas si no se les monitoriza adecuadamente. Los responsables de informática deberían monitorizar la actividad de la red, especialmente el uso de dispositivos portátiles como iPods, memorias USB, etc. Seguramente ninguna empresa querrá que sus datos se vendan a la competencia por un empleado airado.

MÁS MARGEN DE ERROR QUE NUNCA

Resulta irónico pensar que con cada nuevo avance tecnológico, el administrador informático tiene que soportar la carga de una nueva tarea y otro problema más del que ocuparse. Esta correlación se está fortaleciendo a medida que pasa el tiempo y pone de manifiesto las dificultades a las que se enfrentan los administradores informáticos que disponen de presupuestos limitados y falta de apoyo adicional en términos de Recursos Humanos.

El guión de la seguridad informática también ha cambiado. Hasta hace poco, un administrador informático de una pyme estaba concienciado ante todo con los virus y el spam. Sin embargo, hoy en día debe encargarse no sólo de los virus y los correos spam, sino también de la gestión de vulnerabilidades, las revisiones de la red informática, el archivo de e-mails, la gestión de sucesos, entre otras muchas tareas. Para ello, el administrador debe hacer frente a un problema sobre el que tiene muy poco o ningún control: el comportamiento humano.

Las personas son el eslabón más débil en materia de seguridad y por ello, los administradores deben combatir todo tipo de ataques dirigidos a la naturaleza humana – exceso de confianza, falta de conocimiento y credulidad. Todos ellos son factores decisivos para que la seguridad de la red consiga el éxito en los años venideros.

Por otro lado, las compañías se han vuelto totalmente dependientes de la tecnología para hacer negocios de una manera mejor, más rápida y sin límite de fronteras. A su vez, los administradores tendrán que afrontar mayores retos frente a los cuales deberán demostrar su habilidad para proteger de forma adecuada las redes corporativas. La experiencia demuestra que mantener y mejorar la seguridad no resulta una tarea sencilla. Los hackers, creadores de contenido malicioso, spammers y otros elementos, en su mayoría impredecibles, se suman a los factores que provocan a estos profesionales más de un quebradero de cabeza.

Sin embargo, los hechos y las cifras indican que los retos actuales y futuros no provendrán de la tecnología propiamente dicha, ya que por su naturaleza es un elemento neutral que puede usarse tanto de una manera beneficiosa como perjudicial. La mayor amenaza a la que deberán enfrentarse las empresas en los próximos años será la misma que ha azotado al mundo en los últimos 200.000 años: el Ser Humano. Las debilidades, incongruencias y curiosidad de las personas serán explotadas para causar estragos en las organizaciones.

Así que siempre que se levante un dedo acusador sobre un atareado administrador informático, hay que tener en cuenta que puede ser alguien de la plantilla la razón por la que haya cometido un desliz.



David Vella es director de gestión de producto de GFI.