

Protección corporativa contra estafas



Pongámonos en la siguiente situación: un amigo nos dice que en mitad del mar está a punto de emerger una nueva isla. Nuestro amigo nos da todo lujo de detalles sobre la noticia, y al final, nos dice muy serio: “Lo han dicho por televisión”. Si es así, todo debería ser cierto, si lo ha dicho la televisión...

Generalmente esas afirmaciones pueden tener visos de ser ciertas, y en función del amigo que nos la cuente deberemos tener muchas reservas a la hora de afirmar que son ciertas. Puede que haya visto un episodio de ciencia ficción, o que haya visto una información sobre la isla Graham, Ferdinanda o Giulia (según la fuente cambia el nombre). Puede que no tenga ninguna base, o puede ser completamente cierto.

En muchas ocasiones, demasiada gente lo considerará cierto “si lo ha dicho la televisión”, como cuando hace unos 20 años alguien me dijo que habían descubierto una bacteria que destruía los ordenadores (de esa noticia al primer virus informático hay un largo trecho). Afortunadamente otro grupo numeroso de personas pone en la zona de “dudoso” determinadas afirmaciones hasta que pueden verificarlas por algún medio.

Pero estamos en la puerta del año 2007, la experiencia de los rumores ha cambiado. Aunque dudemos de algunas cosas, “lo he visto en Internet” es la nueva frase de moda. Todo aquello que se vea a través de una pantalla y muestre alguna información, es cierto. Aunque lo que me haya llegado por correo sea descabellado, como ha llegado “por Internet”, es válido. Esta manera de pensar va a provocar numerosos problemas a los usuarios de los ordenadores, y muchos más a los administradores de red en el año 2007.

Para los usuarios, el problema más importante en el año 2007 va a ser el de las estafas a través de Internet. La más conocida es el ya clásico “phishing”. Si un usuario crédulo recibe un correo de su banco, sin dudarlo accede allí donde le digan y dejará datos personales suficientes como para que su cuenta corriente se vea seriamente comprometida. Pero usuarios de este tipo quedan cada vez menos, la información va calando, lentamente, entre los internautas. E incluso los bancos son conscientes de estos problemas y en algunos casos (dignos de elogio) avisan a los usuarios de una posible estafa en sus cuentas bancarias.

Por otro lado, los administradores de red se van a encontrar con el mismo problema de estas estafas, pero en dos vertientes muy distintas. Por un lado, tienen que evitar que estos robos se produzcan a nivel corporativo, de manera que el robo de dinero no se produzca en las cuentas de la empresa, sin duda mucho más jugosas que en las de los usuarios (por lo menos en su término medio).

Pero indirectamente también deberá proteger a los usuarios crédulos de su red. Ellos son los responsables de que los contenidos que penetran en la red no sean peligrosos no solo para la información (los virus, gusanos, etc), sino para los usuarios de la red. La protección no es directamente empresarial, sino que se están protegiendo los bienes de los empleados. Un valor añadido de lo que muchas veces no se percatan los administradores corporativos.

Protección corporativa contra estafas



Pero a pesar de eso, siempre puede haber un código malicioso dentro de nuestros sistemas que esté causando problemas. Ese vídeo humorístico descargado por un usuario puede necesitar algún códec ubicado en alguna página maliciosa, de manera que al descargarse e instalarse esté también instalando un troyano. Pero no uno conocido, sino uno exclusivo, del cual se hayan distribuido muy pocos ejemplares en Internet. De esta manera, su detección se volverá muy complicada para los sistemas clásicos. Si la red en cuestión está equipada con sistemas de detección proactiva, estas amenazas de difícil detección podrán ser detectadas.

En un sistema personal, no es excesivamente difícil tener un sistema de protección más o menos adecuado. Todo depende de los conocimientos del usuario: si es consciente de los riesgos que corre, podrá instalar una solución para cada uno de los problemas, incluido el de la detección de códigos desconocidos.

Sin embargo, la instalación de sistemas de protección en un entorno corporativo supone un problema: ¿hasta qué punto está la red en peligro? ¿Estoy evitando las amenazas que puedan llegar a mis usuarios de una manera correcta? Si un usuario no tiene una protección correcta, puede que sufra algún tipo de problema “clásico”, como la desaparición de archivos o la imposibilidad de arrancar un sistema (que a día de hoy es un problema casi menor). Pero si el fallo en la instalación de seguridad supone que pueda entrar en el sistema un mensaje de correo electrónico que intente estafar a un usuario de la red, el problema es mayor. Y muchísimo mayor si ese posible usuario estafado es el responsable de las cuentas corrientes de la empresa.

A la hora de proteger toda una red, no solo hay que pensar en instalar un antivirus y listos. La protección, de manera global, debe considerarse también para las posibles estafas y timos, todo de manera centralizada y con claros sistemas de gestión del riesgo.

Fernando de la Cuadra
Editor Técnico Internacional
Panda Software (<http://www.pandasoftware.com>)
E-mail: Fdelacuadra@pandasoftware.com