


 Reporte

# Seguridad SOCIAL

Establecer pautas claras para el uso de las nuevas tecnologías y de la Web 2.0 dentro del ámbito corporativo se está convirtiendo en uno de los factores clave a tener en cuenta entre las prioridades de seguridad informática.

Por Vanina Lombardi

La seguridad es un viaje y no se puede estar ciento por ciento seguro porque siempre hay cosas nuevas", sentencia George Tsantes, responsable de seguridad informática de Ernst & Young, y considera que "lo más importante es mirar la información sensible, hacia dónde está yendo y quién la está usando... ya no se puede confiar sólo en firewalls y en cerrar puertas".

Así como fue evolucionando la tecnología, también se han modificado los usos que las personas hacen de ella. Los usuarios que antes sólo tenían casillas de e-mail hoy participan en diversas redes sociales, algunas personales y otras más específicas relacionadas con sus trabajos; el intercambio de información y datos se ha multiplicado y la división entre la información laboral y personal comienza a diluirse y suele mezclarse en un mismo dispositivo. Paralelamente, así como están cambiando los usos de la tecnología, en términos de seguridad informática también se han diversificado las formas de actuar de quienes buscan nuevas vulnerabilidades y formas de ataque. "Los delitos cibernéticos se están tornando más profesionales y sofisticados —agrega Tsantes—. La tendencia es obtener dinero directamente, en lugar de bienes que deben venderse para monetizar el delito."

Según la última encuesta global sobre seguridad de la información de Ernst & Young, realizada entre alrededor de 16.000 empresas de más de 56 países, "el 60 por cien-

to de los encuestados percibieron un incremento en el nivel de riesgo que deben enfrentar debido al uso de las redes sociales, los servicios en la nube y los dispositivos personales en las empresas".

Ante esta nueva situación que sigue evolucionando, lejos han quedado los días en que los tradicionales antivirus eran un método suficiente para protegerse. Hoy, es necesario contar con diversas soluciones de seguridad que protejan los datos y bienes físicos, no sólo de la empresa sino también de los empleados.

El reporte de Seguridad Anual de Cisco 2010, en tanto, revela que "los delincuentes cibernéticos están invirtiendo dinero y esfuerzos en 'mulas de dinero' y que los usuarios continúan siendo presas de múltiples maneras de explotación de la confianza". En este sentido, el informe agrega que la mayoría de los delitos cibernéticos no sólo depende de la tecnología, sino también del uso que de ella hacen las personas, y enumera "siete debilidades mortales" que los ciberdelincuentes explotan a través de estafas de ingeniería social: la atracción sexual, la codicia, la vanidad, la confianza, la pereza, la compasión y la urgencia.

Asimismo, la curiosidad (y el morbo), así como ciertos temas de actualidad, también pueden convertir a los usuarios en presa de delitos. Por ejemplo, según un informe de Panda Security, "la dirección web con mayor número de bloqueos preventivos en el primer trimestre de 2011,

para evitar que los usuarios se infectaran, es un link en portugués que ofrece en exclusiva un video emitido por el consulado japonés sobre los efectos del tsunami".

Al respecto, Bob Hansmann, Senior Technology Evangelist de Blue Coat, afirma que "durante las dos primeras horas después del tsunami vimos varias docenas de sitios nuevos que nacieron y usaban Google, Yahoo y otros servicios, que si uno los usaba para ver información relacionada con palabras como 'Japón' o 'tsunami 2011' abrían sitios nocivos". En este sentido, el especialista comenta que un tipo de virus puede cambiar y moverse a otros lugares "más de 3.000 veces en un día", y por eso resalta la importancia de contar con soluciones de anti-virus y filtrado para los servicios en la nube, que en lo posible sean diferentes a las de las máquinas de escritorio. "Es un error depender de una única solución para la protección, se deben tener varias", afirma.

#### Enfoque diferente

Para Glen Kosaka, director de Soluciones Estratégicas de Trend Micro, la seguridad podría dividirse en tres grandes bloques: la del centro de datos, la de la red y equipos de escritorio, y la que atañe a todo lo que sea movilidad. Además, sugiere que "antes de implementar políticas de seguridad de datos hay que evaluar dónde están

los datos, quiénes los utilizan, si los empleados pueden subir información a redes sociales y de qué tipo, qué clase de información está permitida y si lo está en dispositivos móviles, por ejemplo".

Con respecto a la seguridad en la nube, el especialista destaca que "se necesita una arquitectura diferente para administrar la protección de datos en los servicios cloud, que incluye que cada empresa administre sus propias claves de encriptación en la nube con otro proveedor", para que pueda controlar sus datos en todo momento, inclusive al cambiar de proveedor del servicio en la nube.

Por su parte, Rafael García, gerente Regional de Producto para América Latina de Symantec, considera que hay que girar el centro de atención de la infraestructura a la información en sí misma. "La gobernabilidad de la infraestructura debe detallar los pasos y los elementos mínimos para que, sin importar qué tipo de dispositivo se uti-



"Los delitos cibernéticos se están tornando más profesionales y sofisticados. La tendencia es obtener dinero directamente"

**GEORGE TSANTES,**  
responsable de Seguridad Informática de  
Ernst & Young

**R** Reporte

lice para la interacción y para el manejo de información, se pueda tener controlado el flujo de datos y la infraestructura", remarca García.

Otro aspecto que no debe descuidarse es el que se refiere a cuidar que los equipos no se conviertan en medios desde los cuales atacar a otros equipos. Según García, se estima que la Argentina es el tercer país de América latina con la mayor cantidad de ataques generados a través de su infraestructura, después de Brasil y México. "No es que sean argentinos los que están armando el código y haciendo el ataque; se trata de que la infraestructura de la Argentina es la que está generando el impacto y se está viendo afectada para llevar a cabo la distribución, ser un puente o bien atacar directamente a otros usuarios".

**El enemigo interno**

Es importante considerar todos estos factores cuando se piensa en seguridad, para evitar situaciones como la que explica Juan Labonia, IT Manager de Ofishop: "El hacker

**"La Argentina es el tercer país de América latina con la mayor cantidad de ataques generados a través de su infraestructura, después de Brasil y México"**

**RAFAEL GARCÍA,**  
gerente Regional de Producto para América Latina de Symantec

más complicado no está afuera, porque en general se van a buscar las mejores soluciones del lado de Internet; pero del lado de adentro normalmente no se toman tantas políticas de seguridad, entonces viene un usuario con un pen drive que encontró en la calle, lo pone en el sistema y pese a que tal vez uno gastó miles de dólares evitando que un hacker pueda ingresar al sistema desde afuera, termina resultando que un usuario propio logra abrir un túnel desde adentro hacia afuera y la red queda totalmente vulnerable".

Ofishop es una empresa dedicada al comercio electrónico y por eso, según Labonia, prestan especial atención a la seguridad en la Web. La empresa utiliza Linux para todos sus sistemas, lo cual aseguran que también les brinda más seguridad, y cuentan con desarrollos propios para asegurar la información de la compañía.

"Ofishop tiene una política de marketing muy fuerte y las redes sociales son importantísimas, por eso el área de Marketing sí tiene acceso a las redes, pero no el resto de los usuarios", comenta el especialista. Y aclara que esta decisión se tomó por una cuestión de pérdida de tiempo y productividad, más que por problemas específicos de seguridad.

Por su parte, Germán Guerriero, jefe de IT de Pramer, explica que en la productora de contenidos para televisión las redes sociales son de libre acceso, aunque es nece-





Foto: Guinness Financial

sario integrarlas a la organización y efectuar un monitoreo de uso excesivo. En cuanto al control de dispositivos móviles, detalla que se realiza a través de un software centralizado y, para contar con seguridad, utiliza soluciones de diversos proveedores como Cisco, Symantec y CA, entre otros.

“En general las medidas de seguridad no son bien recibidas, por no comprender bien los riesgos asociados a la no aplicación de las mismas”, se lamenta Guerrero y deta-

**“Es un error depender de una única solución para la protección. Se deben utilizar varias”**

**BOB HANSMANN,**  
Senior Technology Evangelist de Blue Coat

lla que uno de sus desafíos relacionados con la seguridad es, justamente, “generar conciencia en los usuarios sobre la importancia de la seguridad informática y alinear a la dirección con las políticas de seguridad establecidas por IT”.

Este no es el caso de Ofishop, donde si bien los empleados no tienen acceso a las redes sociales durante el horario laboral, no hubo resistencia a la medida. En palabras del propio Labonia: “La recepción es buenísima; la gente entiende que lo que hacemos es para cuidar sus estaciones de trabajo, porque quieren trabajar bien y siempre intentamos que sus máquinas funcionen de la mejor manera”.

En suma, los esfuerzos de las compañías parecen estar destinados a lograr un manejo inteligente de la información, teniendo en cuenta los beneficios y los riesgos del mundo conectado, ya que hoy la división entre el trabajo y lo personal se mezcla y en ese río revuelto aumentan los riesgos. ■

### Recomendaciones de los expertos

1. Enfocarse en la productividad, no sólo en “bloquear”.
2. Tener en cuenta que la seguridad en las redes sociales va más allá del malware.
3. Recordar que la seguridad requiere una “defensa en capas”.
4. Tener en cuenta la información y el viaje que hace la información, adónde se almacena, quién la puede ver, si se encripta para el transporte.
5. Focalizarse en educación, concientización y capacitación de los empleados.

Fuente: Entrevistas realizadas.