

EDUCAR PARA PROTEGER LA INFORMACION

LOS VIRUS Y LAS FALLAS SON UN PROBLEMA, PERO EL MAYOR RIESGO SON LOS ERRORES Y DESCUIDOS DE LOS PROPIOS USUARIOS. CASOS Y CONSEJOS.



Los virus, las fallas en los equipos y los delincuentes informáticos son algunas amenazas para los datos. Pero el principal problema, hoy, son los propios usuarios.

Los expertos en seguridad informática coinciden en que la ignorancia, los malos hábitos y los descuidos son los mayores responsables de la pérdida de información.

Cómo hacer para no perder la información

Alicia Giorgetti
pymes@clarin.com

Ni el hardware, ni el software, ni los virus, ni los delincuentes informáticos. Hoy, el principal problema de seguridad informática son los propios usuarios. **Malos hábitos, errores y desconocimiento** son las principales causas de la pérdida o robo de datos informáticos, según coinciden los expertos en seguridad informática.

Si las contraseñas están en un papel pegado en el monitor o bajo el teclado; si se comparten y se las crea a partir de datos evidentes, como el día de cumpleaños o el nombre de la mascota; si se trasladan las notebooks y los celulares inteligentes (*smartphones*); si cualquier persona tiene acceso a cualquier PC y puede copiar datos a un dispositivo USB... **Algo puede andar mal en breve.**

Hace un tiempo, los riesgos para la seguridad informática provenían del exterior de una empresa. Virus, troyanos, gusanos, spyware, ataques de denegación de servicio e intrusiones eran sólo algunos de los riesgos. Ahora, los expertos dicen que los principales problemas de seguridad son la fuga y el robo de datos, y derivan del desconocimiento o mal uso de la tecnología. **El enemigo está adentro, cuidado.**

Se llama fuga de datos a la pérdida de la confidencialidad de la información por extravío, desconocimiento o mala intención. Las principales vías de fuga son los dispositivos USB (*Pen Drive*), el e-mail y la mensajería instantánea.

Ahora la buena noticia: según Bill Robbins, vicepresidente senior para las Américas de Symantec, "el 70% de los problemas internos de pérdida de datos no son intencionales. Se deben a que alguien olvidó una notebook en un taxi o dejó la PC prendida y con las aplicaciones abiertas".

Pero aunque no haya mala intención, igual hay perjuicios, porque se pueden perder datos propios y de terceros (clientes, proveedores, socios, etc.), lo que implica una mayor responsabilidad.

SIN ARREGLO. SI UNA NOTEBOOK SE ROMPE SE ARRIESGA TODA LA INFORMACION.



Sí //

- Capacitar a los empleados y capacitarse.
- Establecer políticas de seguridad interna.
- Fijar reglas para backup y para el uso de las PC.
- Limitar el uso de dispositivos USB.

No //

- No abrir adjuntos en mails desconocidos.
- No cliquear sobre enlaces Web que llegan por mails desconocidos.
- No crear contraseñas basadas en datos personales ni compartirlas.

El perjuicio interno es claro: los datos son necesarios para facturar, hacer marketing, preventa, presupuestos, y más. Y si alguien los encuentra puede cometer un delito como vaciar la cuenta bancaria, por ejemplo.

Reglas y prevención

Hay una categoría de software muy nueva que se orienta a la **Prevención de Pérdida de Datos** (*Data Loss Prevention* o DLP, en inglés). El sistema ofrece reglas para controlar el uso y la transferencia de datos confidenciales dentro de una red corporativa y

hacia dispositivos móviles. Básicamente, la protección de datos involucra tres acciones: **evitar accesos no permitidos a las computadoras, respaldo de datos y protección de las comunicaciones.**

Con el uso creciente de notebooks, palmtops, *Pen Drives* y celulares con capacidad de almacenamiento, es cada vez más fácil copiar datos desde una computadora. Así, bases de clientes, datos financieros y de propiedad intelectual, y planes de negocio y marketing pueden filtrarse sin que nadie se entere. Aunque no haya mala intención, esos datos



MAURICIO NEVAS

PROBLEMA. ANA SABELLI, DE QKSTUDIO, UNA FIRMA DE SOFTWARE, RECUERDA QUE SE LE FILTRO INFORMACION.

no estarán seguros en equipos que se pierden fácilmente.

La historia puede terminar con robos de identidad, dinero de cuentas bancarias o secretos comerciales en manos de la competencia o simples delincuentes. Una alternativa es instalar el software para bloquear el uso de puertos USB y fijar políticas de seguridad con estrictos permisos de acceso.

En QKStudio, una firma que desarrolla aplicaciones sobre Internet, se filtró información de la gestión de proyectos. Ana Paula Sabelli, su socia gerente, recuerda: "La información generada durante la aprobación de un proyecto (el alcance, la propuesta, el presupuesto, etc.) estaba dispersa en los mails intercambiados y las PC de las personas involucradas. No estaba guardada en ningún lado. Al aprobarse el proyecto, esa propuesta se le pasaba a los que debían desarrollarlo, y sólo se borraba el precio. Pero algunos usaron esos datos para presupuestos propios".

Para esto, hay software de gestión de proyectos gratuito y fácil de usar. En QKStudio están implementando el programa Dot Project y, también, trabajan con varias contraseñas que limitan al acceso a los datos. "El uso o robo de datos es imposible de eliminar, pero cuantas más trabas haya, más difícil se hace. Lo importante es definir y escribir procesos para cuidar la información: saber dónde está guardada, que no esté en un servidor con salida a Internet, que las claves no las tengan todos. Si no se sabe definir esos procesos, hay que buscar ayuda", aconseja Sabelli.

En la rosarina NyV SRL, que fabrica bicicletas, le dan mucha importancia a las claves. Cristian Viscobia, socio de la firma, apunta: "La pérdida o robo de datos

El 70% de la pérdida de datos no es intencional. Se debe a que alguien olvidó una notebook o dejó la PC encendida.

“ ”

Con el uso creciente de notebooks, palmtops y celulares, es cada vez más fácil copiar datos desde una computadora.

“ ”

deriva de malos hábitos y de no respetar dos reglas: las claves son personales y no se prestan, y que las computadoras se prendan y apaguen en el día", dice.

El ejecutivo agrega: "Tenemos reglas de selección -no usar nombres de familiares ni fechas personales- y de uso -no prestarlas ni usar la PC de un compañero sin cambiar de usuario-. Si se comparte una PC y no se respeta el uso privado de claves, cuando hay un error no se puede saber a quién corresponde". Hoy la tendencia es reemplazar las contraseñas con otros sistemas de autenticación, como lectores de huellas digitales, que ya vienen en las nuevas notebooks.

Ingeniería social

Una táctica frecuente, y muy poco difundida, es la ingeniería social. En la jerga, el término alude a las técnicas para sonsacar información por medio de artimañas y engaños: es la base del phishing. Una muy difundida es

por vía de mails. Un usuario recibe un mensaje de su banco, por ejemplo, o de una empresa reconocida. El mail tiene una dirección Web que pide datos como el DNI, la dirección física, la contraseña de acceso y el número de cuenta bancaria. El usuario los ingresa sin saber que le están robando sus datos, que luego pueden usarse para cometer delitos.

Otro peligro es la falta de prevención: este año el gobierno de Inglaterra extravió casi 500.000 datos personales de niños, beneficiarios de planes sociales y presos. Se ganó un escándalo público. Y la policía alemana compró un CD con seis millones de datos personales por 850 euros mostrando que hay un mercado ilegal de compra-venta de datos.

Una alternativa para que no puedan usarse los datos perdidos o robados es encriptarlos. La encriptación "enmascara" los datos para que sólo puedan ser leídos por la persona adecuada, con una clave. Se puede usar el software Pretty Good Privacy (PGP).

Ante las pérdidas, por errores o por acciones ilícitas, lo mejor es hacer copias de respaldo o backup. "En 2007 nos robaron los tres estudios de diseño de sonido y pudimos seguir trabajando porque estaba todo respaldado", dice Juan Carlos Varela, director de La Pirada, empresa que diseña sonido para comerciales y programas de televisión.

"En 2001, una computadora se golpeó en un traslado y perdí presupuestos, datos de contacto y fotos, entre más cosas. Ese día decreté que todos los viernes debía hacerse un backup de las 16 PC a DVD. Yo hacía copias a un disco duro externo usando el sistema operativo que permite programarlas, pero dejé de hacerlo y perdí todo porque se me cayó la notebook. Ahí decidí no trasladar

OPINION

Gustavo Aldegani
CONSULTOR EN SEGURIDAD INFORMATICA



Diez claves para asegurar los datos

- ● ■ La seguridad debe agregarse a su computadora, no viene "de fábrica".
- Encripte la información de su disco y sus mensajes de mail. No es difícil, y el software *Pretty Good Privacy (PGP)* es gratuito.
- Lleve sus archivos importantes en un *Pen Drive* y éste en el bolsillo. No lo haga en la notebook. También puede encriptar los archivos.
- Endurezca las palabras claves reemplazando letras por números parecidos. Ejemplo: Gustavo por 6u5t4v0.

- Si deja su PC encendida, active un protector de pantalla con una palabra clave.
- Nadie le pide información personal crítica por mail o por Web. Si tiene dudas, confirme telefónicamente con la entidad que hace la solicitud.
- El antivirus y el firewall personal actualizados ya no son suficientes.
- La notebook debe ir siempre con usted y en un bolso que no anuncie lo que contiene.
- No deje papeles en la impresora e invierta \$ 200 en una destructora. También sirve para destruir todo el correo en papel que recibe y que puede contener datos personales y bancarios.
- Si ocurre algo malo, lo mejor es tener una copia en CD o DVD de sus archivos, lo más actualizada posible.

más la laptop, sólo llevo los archivos", añade Varela. Para minimizar la posibilidad de pérdidas, todos los mails que salen de La Pirada con presupuestos, convenios, archivos de audio y datos confidenciales se copian a dos personas de la empresa.

Proteger las comunicaciones

Las redes sociales, la mensajería instantánea y el uso de redes inalámbricas desde distintos dispositivos son vías posibles de escape de datos. Para evitarlo, se requieren políticas empresariales que fijen su uso.

En la agencia Diálogo Publicidad hay bastante autonomía. Enrique Zeppa, encargado de Sistemas, comenta: "La empresa quiere que si un cliente viene con una notebook pueda conectarse a la red Wi-Fi. Como eso implica un riesgo, fijé contraseñas duras, con caracteres alfanuméricos, pero son difíciles de recordar y todos terminan anotándolas. Además, los empleados tienen acceso a todo porque se cree que lo necesitan para su trabajo".

Y continúa: "Una vez, alguien cliqueó en un mensaje extraño del Messenger aunque estaba en otro idioma. Otro problema es la gran rotación de personal que hay en las agencias de publicidad. Si alguien se va, hay que verificar que deje de tener acceso a la red interna. Muchos creen que las computadoras y las redes funcionan como la electricidad o el televisor, pero no es así".

Para montar una estructura segura para la información, la primera recomendación del ejecutivo es tomar la decisión política. "Luego se pueden hacer cosas que no demanden tantos recursos; por ejemplo, usar funciones que vienen en los sistemas operativos y concientizar a los usuarios", concluye.



DATOS UTILES

Cómo usar el Pretty Good Privacy (PGP)

Quiere decir "privacidad bastante buena". Es un programa cuya finalidad es proteger la información que circula por la Web, mediante el uso de criptografía de clave pública. Se trata de un programa informático gratuito que, usado en forma correcta, puede proporcionar un alto nivel de seguridad.

Web para descargar: www.derechos.org/nizkor/pgpinstr.html

TrendProtect

Es otro software de seguridad gratuito que se adjunta al navegador Web y que impide a los usuarios el ingreso a sitios y páginas de Internet cuyo contenido resulte dudoso.

Web para descargar: www.trendsecure.com/portal

Dirección Nacional de Protección de Datos Personales (DNPPD)

Es el organismo estatal encargado de controlar la utilización y el contenido de las bases de datos que almacenan información de las personas.

Web: www.jus.gov.ar/dnppd