La inseguridad también afecta a la Red

En la actualidad, los virus que ingresan en las computadoras y las intromisiones ajenas para obtener información privada en los equipos son un delito común. La seguridad informática resulta de vital importancia para contrarrestar sus efectos.

PorAldegani Gustavo

Las nuevas tecnologías desembarcaron no sólo con un listado infinito de beneficios para sus usuarios. Los daños y perjuicios a los que están expuestas las computadoras y redes en las que operan activaron anticuerpos que ayudan a mantenerlas seguras, aisladas de virus y odiosas intromisiones.

Los ***hackers*** se identifican como empleados de una determinada compañía o ***call center.*** Seducen con la charla hasta que consiguen el nombre de usuario y su clave.

Pues bien, la seguridad informática –pues de ella se trata- es "el conjunto de acciones que les permite a los negocios, basados en las computadoras, llevar adelante sus tareas de manera segura", explica Gustavo Aldegani, consultor independiente, con 25 años de experiencia en la implementación de sistemas seguros en empresas, organizaciones militares y gobiernos de la Argentina, distintos países de América Latina y los Estados Unidos.

Sus comienzos se remontan, en simultáneo, la puesta a punto de la primera computadora, durante la década de 1960, cuando la NSA de los Estados Unidos publicó los primeros documentos sobre Seguridad Informática, algunos de los cuales, en la actualidad, se conocen como *Rainbow Books.* En los años 90 dicho paradigma se actualizó luego de que un grupo de investigadores trabajara sobre nuevos escritos que modificaron a los originales.

¿Quiénes necesitan seguridad informática?

Todas aquellas personas que tienen una computadora. Los beneficios son múltiples y comunes para las empresas y los usuarios particulares. En el caso de las compañías, porque se benefician al operar de manera más segura, mientras que los particulares conectados a Internet sufren menos ataques de virus en la medida en que tengan en su equipo un antivirus que lo proteja. Eso no sólo mantiene segura y aislada a la computadora, sino que también evita que el virus se propague hacia otras máquinas.

¿Qué importancia le prestan las empresas al tema en particular?

En el caso de las compañías cuyos negocios principales dependen de sus computadoras, es fácil imaginar la trascendencia que le dan: mucha. Ya no sólo disminuyen riesgos objetivos, sino que cumplen con determinados estándares de seguridad a partir de las exigentes normas internacionales que imponen las empresas que compran servicios informáticos.

¿Qué costos tiene implementar un sistema de seguridad en una compañía?

En su presupuesto destinado a la tecnología, una empresa que maneja su seguridad informática de manera confiable debe destinar entre el 10 y el 40 por ciento a productos y servicios de seguridad.

La confianza puede significar el principal enemigo que encuentra la seguridad informática a partir del desuso de las máquinas o los pocos inconvenientes que les generaron los virus a los usuarios más afortunados. Sin embargo, Aldegani insiste

Entre el 10 y el 40 por ciento del presupuesto destinado al área de tecnología de una empresa debe destinarse a la seguridad informática.

en que "siempre" es necesario contar con un sistema de protección. "Su complejidad será similar al negocio que tienen los sistemas a asegurar", afirma el experto. Por otra parte, aclara que en dicho ámbito existe un nivel estándar entre todos los países respecto a la calidad de sus productos: "Si una PyME argentina quiere venderle servicios a cualquiera de las grandes, debe cumplir con estándares de seguridad comunes a todos los países informatizados, debido a que las casas matrices mantienen políticas muy estrictas de contratación que alcanzan a sus operaciones en todo el mundo".

¿Cómo influyó la llegada de Internet respecto a la seguridad informática?

Su llegada tuvo un alto impacto. No sólo porque es una fuente de riesgos en sí misma, ya que es una puerta a la que todos pueden acceder, sino que además es un medio de dispersión de programas dañinos y medio de comunicación de técnicas maliciosas.

¿Existe en la Argentina legislación vigente sobre este tema en particular?

Funciona la Ley de Delito Informático, la de Protección de Datos Personales y la de Firma Digital. No obstante ello, los países que toman al asunto como un elemento de primera necesidad modificaron su equivalente a nuestro Código Civil. Allí se preocuparon más en incorporar los conceptos necesarios para actuar legalmente en el ámbito digital que en tener una legislación específica para los delitos.

El Consejo apuesta a la prevención de los delitos informaticos.

El Área de Seguridad informática del Consejo evitó, tiempo atrás, un ataque informático anónimo que pretendía involucrar a la matrícula. A través de un correo, se les solicitaba a los matriculados la identificación de usuario y la clave para ingresar a las casillas personales a fin de "hacer una depuración a partir de problemas existentes en el disco".

"Ese fue un caso de phishing, uno de los delitos más clásicos", explica el Lic. Carlos Freyre, gerente de Seguridad Informática de nuestra institución. Y continúa:"Se trata de una manera fraudulenta de engañar a un usuario para capturar algún dato y con esa información personalizarse como dicho usuario. Para llevar adelante una maniobra ilícita.

Lic. Carlos Freyre

¿Se necesita algún software para hacerlo o basta con la sola confianza?

Lo que hace que sea una práctica habitual es que no necesita software ni una técnica especial, sino la confianza que uno tiene para hablarle a la otra persona y para que ésta se sienta cómoda y brinde sus datos personales. Por lo general, se identifican con correos electrónicos pertenecientes a una empresa/organización, o como empleados de una determinada compañía o de un c*all center.*

Para solucionarlo, ¿es necesario reconfigurar todos los accesos?

Depende del daño que causó. Existen casos en que se llevan un dato puntual del usuario y sólo basta con modificar los perfiles de acceso de esa cuenta. Si uno reacciona inmediatamente después de haber entregado los datos y tiene el tiempo suficiente para cambiar las claves, por ejemplo, se podría salvar la información que estuvo expuesta.

Desde el punto de vista tecnológico, ¿existe alguna manera de prevenirlo o es inevitable?

La mejor prevención es la concientización de los usuarios. Prevenirlos sobre estas maniobras para que estén atentos es la mejor opción. Pasa en el ámbito cibernético, como así también en el personal; el *modus operandi* es similar. Por ejemplo, cuando se identifican como policías en la puerta de tu casa y después ingresan a robarte.