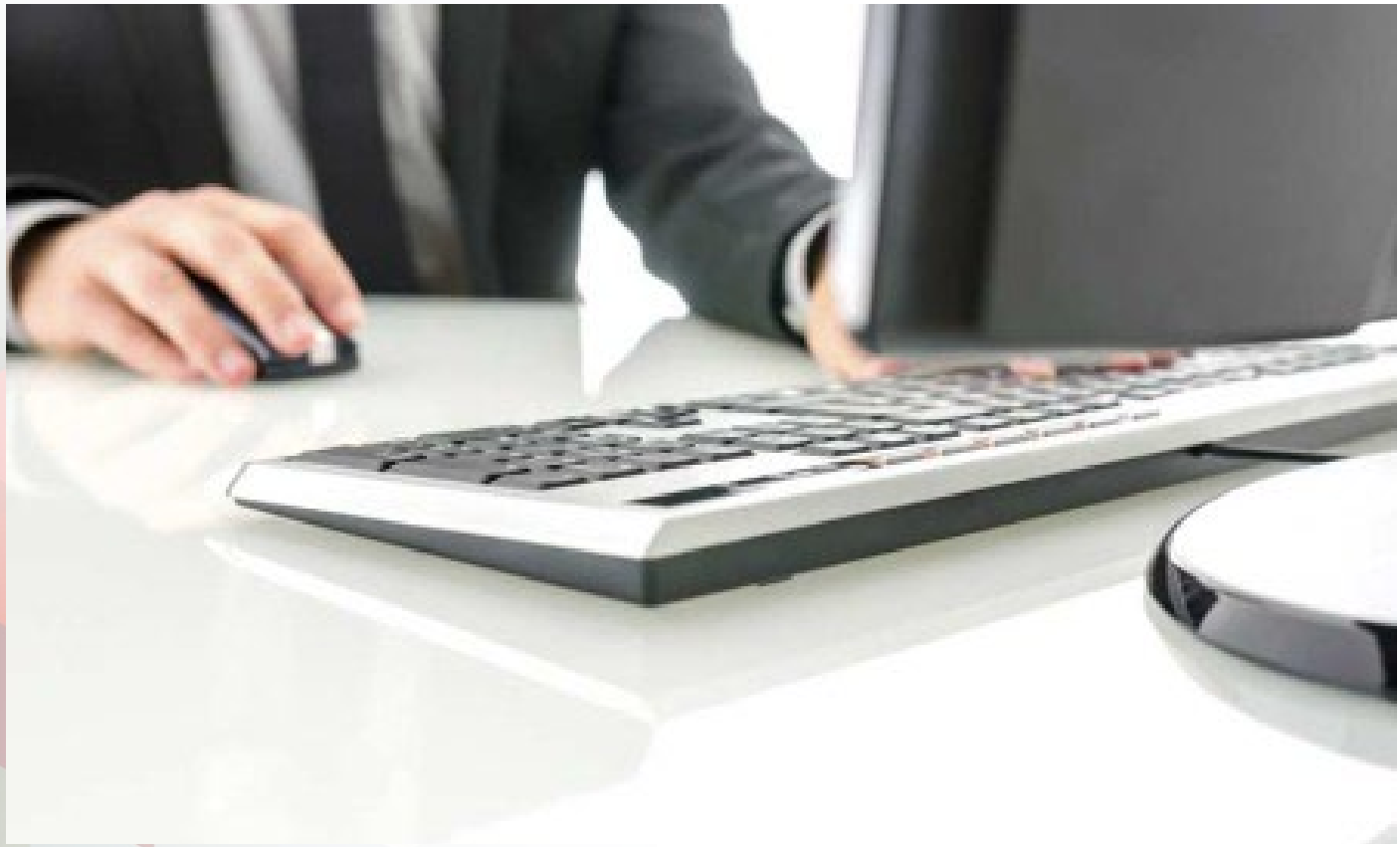
Los peligros de la informática, donde el riesgo se hace evidente

FRANÇOIS SETTEMBRINO

¿Es este un título atractivo dirigido únicamente a llamar la atención del lector o, por el contrario, corresponde a una visión realista de la situación? Estamos hasta tal punto sumergidos en la informática con los dispositivos, los contactos, los correos electrónicos y otras redes que se nos cruzan en el camino, que no nos damos cuenta de nuestra dependencia literalmente enfermiza. Los expertos en medicina nos animan a desconectar con regularidad para evitar poner en riesgo nuestra salud, y a ocuparnos, en primer lugar, en extremar la vigilancia en el trabajo, al volante o a centrarnos en las verdaderas relaciones sociales; su única preocupación es ayudarnos a conservar un equilibrio vital que, de otro modo, correría el riesgo de desaparecer deprisa y sin darnos cuenta, como hemos dicho, a causa de los dispositivos que utilizamos. Esta preocupante cuestión se extiende a muchos más ámbitos de los que imaginamos y sobre los que vamos a abordar modestamente algunos aspectos.

Comenzaremos por una fecha: 8 de abril de 2014. Fue cuando Microsoft se desvinculó de Windows XP; a partir de entonces, se acabarían las actualizaciones de seguridad y el soporte técnico. Microsoft no tiene intención, por tanto, de llevar el mantenimiento de por vida de un programa que ha cumplido su cometido y ha sido reemplazado por otras versiones con mejores prestaciones. ¿Pero estamos a tiempo de modernizar los viejos ordenadores? Sin duda, verse obligado a adquirir nuevos equipos puede salirse del presupuesto. Algunos equipos podrían actualizarse, pero su uso no sería sencillo precisamente. En muchos otros casos sería imposible, debido a la falta de capacidad de los dispositivos, y los problemas por tanto se acentuarían con el paso del tiempo. La situación es más grave de lo que parece. Muchos particulares ya han decidido correr el riesgo y continuar utilizando XP, porque carecen de los medios necesarios o no les apetece realizar una nueva adquisición. En las empresas, podría ser aún peor. En Gran Bretaña, tan solo en el sector de la sanidad, más de un millón de dispositivos funcionan con XP… Parece asimismo que la mayoría de los distribuidores de billetes de banco en todo el mundo estaría en la misma situación. Todo esto, salvo que se exija a Microsoft revisar o atenuar su postura, podría quedarse en buenas intenciones, y cuanto más esperemos, peor. De todas maneras, recordemos que habría más de mil quinientos millones de ordenadores en el mundo, de los cuales más del 90 % funcionan con Windows. No todos tienen instalado XP, pero debe haber todavía un gran número de ellos que satisfacen las necesidades de los usuarios. Aquellos que todavía se usan en las empresas, principalmente en el caso de las PYMES, deberían modernizarse o sustituirse lo antes posible para mantener un nivel de seguridad adecuado. En estos casos, habrá que contar con especialistas, que trabajarán gratuitamente.

La seguridad de los dispositivos de particulares también está en juego; la banca por Internet puede convertirse en un blanco certero para los malhechores, y los banqueros podrían igualmente denegar el acceso a clientes con XP para protegerse. Las personas que tengan un técnico de confianza, deben contactar con él cuanto antes. En su defecto, podrán hacer uso de los servicios de un profesional a cambio de una protección que, de todos modos, nunca será definitiva.



CUESTIONES A CONSIDERAR

¿Qué otras cuestiones habremos de vigilar, temer o sufrir? Las siguientes consideraciones no son más que unos pocos ejemplos entre tantos. Hay algunos que nos pueden resultar relativamente familiares por lo que se publica en los medios; otros los conocemos más en profundidad, gracias a ciertas revelaciones, entre las cuales destacan las declaraciones de Edward Snowden, el antiguo empleado de la CIA en las que divulgó parte de sus documentos clasificados como secretos.. Todo comienza con un saqueo de datos a través de la utilización de un correo electrónico. Más discreto es el procesamiento de contratos por servicios de traducción en línea que, si se piratean o están infectados, permitirían a la competencia estar al tanto de todo casi inmediatamente. La propiedad intelectual carece de sistemas de protección eficaz y los países occidentales europeos ya no tienen secretos para nadie; sus economías están en peligro. En la base de todo se halla la ausencia de una regulación eficaz en materia de datos; cuando las primeras tarjetas de fidelidad comenzaron a proliferar en las tiendas, nadie quiso ver la artimaña cuyo fin sería el uso de los datos personales de los clientes para obtener información detallada sobre ellos. Se ha alabado la protección de datos personales, los cuales tenemos el derecho de conocer para corregirlos a voluntad. ¿Pero cuántos se han aventurado a hacerlo? Si es usted cliente de una cadena internacional, desconoce por completo el uso que se hace de sus datos personales que, al parecer, poseen un valor inestimable. Los ficheros de las grandes cadenas de tiendas permiten disminuir la parte aleatoria de las decisiones de compra, pues se conoce casi todo sobre el perfil del cliente; si además se suman las huellas digitales que vamos dejando con las tarjetas, los teléfonos donde todo está registrado, las visitas a las redes sociales, los correos electrónicos, de vez en cuando un historial médico, incluso el GPS, estamos facilitando información susceptible de utilizarse para hacerle caer en la trampa. No olvide tampoco los millares de cookies que dejan un rastro imborrable y que contienen gran cantidad de información sobre usted; estas permiten seguirle la pista, detectar sus preferencias y reconstruir su comportamiento. Google no pierde ocasión para alabar los beneficios de las cookies, pero en breve las remplazará por un identificador anónimo, más eficaz e insidioso, del cual será el único propietario.

Usted ya no tendrá por tanto opción a interactuar. Y con el tiempo los comercios e industrias que no utilicen el navegador Chrome de Google se encontrarán dando palos de ciego y ya no podrán personalizar su publicidad. Así, pues, como individuos, casi nada nos pertenece, nada es nuestro ni es secreto; si no ocurre ahora, llegará el momento en que nuestros datos personales y el rastro que dejamos serán utilizados permanentemente, ya sea para un contrato de trabajo, un seguro, un asunto judicial, etc. Además, toda esta información va a parar a empresas, Google y tantas otras, reguladas por legislaciones y tribunales extranjeros. Y aquel de entre nosotros que quisiera hacer desaparecer algún dato de su historial, habrá perdido el poder para hacerlo. Se ha puesto muy de moda tener un perfil en Facebook o en cualquier otra red social, sin comprender que la revelación de la vida privada no puede más que volverse contra uno mismo. En caso de litigio, solo cabe desear buena suerte al que quiera llevar el asunto ante los tribunales, en particular los estadounidenses, ya que las principales empresas se encuentran reguladas por la legislación de EE. UU. No nos olvidemos tampoco de que para beneficiarse de su protección legal, también hace falta ser ciudadano estadounidense.

HISTORIA RECIENTE

Repasando un poco la historia, recordemos que fueron los militares de Estados Unidos quienes fomentaron el auge de la informática personal, o los PC, si se prefiere. Pocos saben que la palabra Informática es un acrónimo de dos vocablos, INFORmación y autoMÁTICA. Y en efecto, con el desarrollo de los ordenadores que son cada vez más potentes y de una rapidez vertiginosa, dotados de memorias virtualmente infinitas, ha hecho casi automática la posibilidad de hacerse con datos confidenciales, incluso los más secretos, y ha permitido una vigilancia universal. El problema radica en que de nuevo son los militares estadounidenses los se han reservado todos los poderes.

A su vez, el poder de la maquinaria estadounidense no cesa de crecer. Sus dispositivos serán capaces de colarse en secreto prácticamente en todas partes. En primer lugar, en nuestros datos particulares, a través de la «puerta trasera» de los ordenadores y en cualquier organización, incluida la policía. La potencia de sus dispositivos será tal, que les permitirá eliminar parámetros ínfimos de cualquier sistema o red, industrial o militar, con el fin de dejarlo obsoleto o inoperativo. Son ellos quienes idean conjuntamente sus sistemas de seguridad. La tarea de elaborar una criptografía efectiva corresponde a los grandes especialistas, y no habrá otros capaces de proteger eficazmente a las empresas y a las administraciones. Cuando compramos un ordenador, el sistema pertenece en un noventa por ciento a Windows; ¿y quién nos garantiza que la protección criptográfica que hemos pagado a un alto precio no incorpora un pequeño repetidor que solo el diseñador conoce?

El título de este artículo hace referencia a nuestro nuevo entorno; el riesgo ha dejado de ser aleatorio, y su presencia es una constante. Todos los días recibimos nuevas pruebas de ello; estas son algunas de ellas:

- La agencia tributaria canadiense ha descubierto un fallo en su sistema de cifrado, que implica la posibilidad de haber sufrido el pirateo de los datos de un elevadísimo número de ciudadanos.
- En Bélgica, el sistema informático de SPF Finances parece tener notables vulnerabilidades que comportan fallos a todos los niveles.
- ING ha dado mucho que hablar por querer vender información sobre el comportamiento de compra de sus clientes. La seguridad y el respeto de la vida privada son los grandes perdedores, pues los ficheros de clientes se venden o alquilan a precio de oro.

Estos no son más que algunos ejemplos y es más que probable que ciertos usos ilícitos se practiquen impunemente y en riguroso secreto. Nosotros, los usuarios, somos igualmente responsables porque apenas unos pocos marcamos sobre los formularios la casilla con la que podemos negarnos a que nuestros datos sean comunicados a terceros.

Desde diversos ámbitos se intenta llamar la atención de los responsables políticos sobre el peligro que comporta no hacer nada. Ni siquiera Europa es capaz de ver el peligro, y no tiene programado ocuparse de la cuestión hasta 2015. Pero, entretanto, las compañías que manejan las redes se embolsan sumas astronómicas, de las cuales apenas veremos aquí unas migajas, que no permitirán la recuperación de nuestras economías. ¿Mejorará la situación al menos para los expertos del Risk Management? El renombrado Institute of Risk Management, de Londres, ha ahondado en la cuestión del cyber risk, como lo llaman; la conclusión es desmoralizadora:

- 360 millones de cuentas bancarias se encontrarían en el mercado y, según KPMG, 160 millones de personas en 2012 habrían sufrido filtraciones de datos.
- El setenta por ciento de los gestores de riesgos carecen de cualificación y experiencia en este campo.
- El cincuenta y tres por ciento de las sociedades encuestadas carecen de gestión alguna de la materia.
- Un modesto veintisiete por ciento ha estudiado la totalidad de las medidas de seguridad incorporadas en sus cadenas de suministro.
- Y como si todo esto no fuera suficiente, el cuarenta y cinco por ciento de los encuestados ignora si su empresa ha sufrido ya ataques cibernéticos o daños.

¿Podemos hacer algo, considerando que la urgencia apremia? Aquellos que quieran profundizar en la cuestión no pueden contentarse con la lectura de este breve artículo. He aquí dos pistas que pueden guiarlos:

- Primero, una obra destacada en francés: La souveraineté numérique (Stock, 2014), de Pierre Bellanger, que realiza un recorrido por la cuestión.
- Después, un resumen y el informe Cyber Risk, del IRM, en inglés, que se pueden consultar en la web del instituto (www.theirm.org). ■

CONCLUSIONES

¿Y quién tiene la culpa de que el riesgo se haya convertido en una realidad? En primer lugar, nosotros mismos que nos hemos zambullido de lleno en redes sin ponderar adecuadamente los peligros; después, los responsables informáticos que no han sabido medir estos peligros. Pero también los gestores del riesgo, que se han quedado atrás y no han sabido reaccionar a tiempo. Son ellos quienes deberían haber educado a sus superiores y dirigentes, estos últimos aún más responsables por no haberse preocupado apenas por el fenómeno. La esfera política se ha quedado desfasada, cuando debería haber anticipado las catástrofes que nos esperan.

Dejemos que sea Pierre Bellanger quien diga la última palabra:

"Internet y sus servicios están controlados por los americanos. Internet trasvasa nuestros empleos, nuestros datos, nuestra prosperidad, nuestra fiscalidad, nuestra soberanía".

Esto es lo que se sabe con certeza hoy por hoy; para merecer su título, los gestores de riesgo están en la obligación de reaccionar. Y ya va siendo hora.