Seguridad informática… algo más que antivirus

[:es]

Autor: Yaditza del Sol González | yadidelsol@granma.cu

16 de febrero de 2017 22:02:06

En Cuba también somos sensibles a las vulnerabilidades de los sistemas operativos mundiales, ya sean Microsoft, Android o Mac OS

Robo de información; tráfico de datos; herramientas remotas para tomar el control de una computadora; sitios web falsos que esconden programas malignos; suplantación de identidad en las redes sociales; ataque a las comunicaciones y servicios públicos…, tal parecería que estamos narrando la trama de una película hollywoodense, de esas donde los hackers malos toman el control de una red del gobierno y el policía bueno llega a tiempo, casi en el último minuto, para salvar el mundo.

Y sin embargo, hay cierta verdad en lo ficticio.

Quitando el trasfondo teatral y casi risible del argumento, no estamos tan lejos de ese día como quizá imaginamos. Nuestra sociedad, cada vez más (de) pendiente de las tecnologías, ha creado la brecha perfecta para que hasta un niño de 12 años escriba códigos informáticos y pueda hackear cuentas en sitios de juegos.

¿Pero qué tiene que ver esto con nosotros?, ya se preguntarán algunos. Bueno, mucho más de lo que creen.

La seguridad informática es un término conocido para cualquier país, y Cuba no es la excepción de la regla. Aquí también somos sensibles a las vulnerabilidades de los sistemas operativos mundiales, ya sean Microsoft, Android o Mac OS, sin mencionar que las redes institucionales se ven constantemente «bombardeadas» por correos electrónicos de dudosa procedencia y por los llamados spam (e-mails no solicitados que se envían a un gran número de destinatarios con fines publicitarios o

comerciales).

Entonces, sí. Hay que hablar de protección de datos, de antivirus, de controles de acceso y análisis de riesgo, ya que la respuesta nunca estará en impedir el uso de los medios de informatización o frenar el desarrollo, sino en aprender cómo protegerse ante las alteraciones que se dan en el ámbito digital.

«En la medida en que se perfeccionen las tecnologías de la información y las comunicaciones (TIC) y sus aplicaciones se extiendan a todas las esferas sociales, se torna más importante establecer ordenamientos jurídicos, y no solo para sancionar delitos, sino porque hacen falta normas que velen por su correcto empleo.

«Desde este punto de vista, el manejo de los datos necesita de regulaciones, de otra forma, la información —que se convierte en el activo más preciado de la entidad— puede estar al alcance de personas no autorizadas o ser utilizada con fines indebidos», explica a Granma Gonzalo García Pierrat, director de organización y control de la Oficina de Seguridad para las Redes Informáticas (OSRI).

En tal sentido, lo más acabado que tiene Cuba en materia de seguridad informática no es una ley, sino la Resolución 127 del Ministerio de Comunicaciones (Mincom), emitida en el 2007; un documento que establece algunos procedimientos básicos para minimizar los daños en sistemas informáticos, además de regular el uso de las TIC en las entidades.

Sin embargo, ya han pasado diez años; y en lenguaje de las tecnologías, lo más viejo fue lo que salió en el mercado la semana pasada. Por ejemplo, algunas medidas resultan hoy tan obsoletas como negar el acceso a contenidos noticiosos porque tal búsqueda no es afín al contenido laboral del usuario.

Si bien está claro que las tecnologías que posee una entidad están dirigidas al objeto social de dicho organismo, y no para beneficio personal, tampoco se trata de negar las cosas porque sí, y mucho menos cuando las TIC pueden convertirse en una puerta a la superación profesional.

«La seguridad informática no existe para evitar que se usen las tecnologías, sino para que su uso sea de la manera más segura posible. Y a veces cometemos el error de prohibir las cosas, porque es más fácil decir no a tener que hacer el trabajo de monitoreo y control», comenta García.

«La Resolución 127 trató de ser, en su contenido, lo más amplia posible, y aunque sigue siendo útil y abarca un conjunto de aspectos importantes, es cierto que han aparecido cambios en el área de la informática y no es todo lo suficiente que se

requiere ahora mismo».

De ahí, informa, que el Ministerio esté trabajando en un nuevo reglamento, en el cual se podrían introducir quizá algunas cuestiones relacionadas con las redes inalámbricas o ampliar las disposiciones para la navegación en la web.

Tal y como plantea Yarina Amoroso, presidenta de la Sociedad Cubana de Derecho e Informática de la Unión de Juristas de Cuba, la seguridad es un proceso de perfeccionamiento continuo, e implica que la reglamentación por la que se implementan y ordenan los usos de datos y servicios, sea sistemáticamente actualizada.

«El objetivo es brindar una protección adecuada contra las amenazas accidentales o intencionadas a la confidencialidad, integridad o disponibilidad de una red; y ello implica también implementar mecanismos para darle seguimiento al cumplimiento de los objetivos de la legislación en términos de eficacia y eficiencia», dice Amoroso.

A FALTA DE UNA LEY…OTRAS SOLUCIONES

Más allá de lo que pudiera ser cambiado o no, lo que sí está claro es que las reglas por sí solas no hacen todo el trabajo; las personas también deben tomar conciencia y saber que son responsables por las acciones que realizan en el ámbito digital.

Tan importante es la redacción de leyes claras y precisas, como la autorregulación del usuario. En ambos casos, Cuba tiene viejas deudas.

Según considera el director de organización y control de la OSRI, uno de los grandes vacíos legales que tenemos ahora mismo es que no existe una vía directa para sancionar a una persona por introducir programas malignos o acceder sin autorización a una red. «Todavía hay quienes consideran innecesario tipificar los delitos informáticos dentro del sistema judicial, pues creen que las infracciones o violaciones cometidas en esta área se pueden, como delitos, juzgar dentro de los estatutos generales».

Y aunque en nuestro país se ha reconocido la pertinencia de hacer esta delimitación, las palabras y buenas intenciones no acaban de concretarse en hechos. «Desde hace más de una década se está discutiendo un proyecto para incluir modificaciones en el código penal cubano, pero mientras se espera la aprobación, los daños continúan», asegura García.

«Al no tener tal tipificación, cuando se presente un caso de delito informático frente al tribunal de justicia, el hecho tiene que ser considerado en analogía con

otra transgresión que se le parezca, como daños a la propiedad económica de una empresa. Entonces por ahí es que se juzga, y no por el delito informático en sí mismo».

Por ejemplo, si un ciudadano crea y propaga intencionadamente un virus informático y no hay daño colateral que se pueda cuantificar, desde lo penal, estamos en desventaja, sostiene. «Casi siempre logramos una condena, pero las complicaciones son muchas cuando la situación pudiera solucionarse de forma más sencilla».

Entre el 2004 y el 2006, rememora García, estuvo circulando un gusano (programa maligno) que afectó a un importante número de empresas, sobre todo en La Habana. No obstante, para demostrar el perjuicio que ocasionó este delito, hubo que visitar a cada uno de los afectados y cuantificar las pérdidas.

«El proceso se hizo más engorroso porque había directivos que no sabían cómo determinar, en cifras monetarias, el daño que significaba para la entidad tener caída durante una semana la red de telecomunicaciones (correos electrónicos, conectividad a Internet, llamadas telefónicas)».

Entonces volvemos, como en efecto dominó, al otro elemento de la cadena: la cultura del usuario. A veces pensamos que por instalar un cortafuego o poner contraseñas ya está asegurada la estabilidad de la red, cuando la educación informática de quienes poseen y usan las computadoras resulta tan determinante como un buen antivirus.

Autentificar el acceso a los datos con contraseñas, no responder e-mails que soliciten información personal, no descargar ficheros de fuentes desconocidas, ni instalar aplicaciones sin ser autorizados, pudieran parecer medidas demasiado básicas como para que alguien no sepa de ellas; y sin embargo, sucede.

Por supuesto, desde lo interno de cada organismo también deben efectuarse acciones de control. Según García, el administrador de la red «tiene que ejecutar un análisis de riesgo y determinar cuáles son las prioridades en términos de seguridad, o sea, de qué virus o fallos hay que proteger los programas y softwares más importantes». Todo ello, agrega, sin descuidar las barreras físicas para preservar los ordenadores y equipos de eventualidades como incendios, terremotos, inundaciones y fallos en la instalación eléctrica.

No obstante, lo que suele suceder casi siempre es que se elabora el plan de seguridad y se implementan los controles, pero no se hace nada más hasta que ocurre un incidente.

Niurka Milanés Sarduy, directora general de la empresa cubana Segurmática, señala

que la supervisión es la primera barrera para frenar cualquier problema en la red. «Soluciones antivirus, antispam, análisis de URL maliciosas, así como mantener actualizado los parches de seguridad pueden hacer la diferencia».

PRODUCTOS Y SERVICIOS 100 % CUBANOS

La empresa Segurmática es la principal gestora de soluciones antivirus en el país. **Foto:** Yaimí Ravelo

Segurmática y la OSRI —cada una con sus roles específicos— son las principales gestoras en el desarrollo de respuestas computacionales en el país, al menos si de seguridad informática se trata.

La primera, con más de 20 años de experiencia, se destaca por su producto líder: Segurmática Antivirus, disponible tanto para personas naturales como jurídicas. «Su finalidad es brindar una respuesta técnica a los programas malignos que circulan en la red nacional y los dispositivos extraíbles de los clientes», asegura Milanés.

La población, precisa, puede acceder a la herramienta a través de su distribuidor nacional que son los Joven Club de Computación y Electrónica, o ir a sus oficinas y contratar personalmente el servicio.

También desarrollamos el SavUnix, un antivirus con funcionalidad en el sistema operativo Linux, y el Segurmática Seguridad Móvil para dispositivos Android 4.0 o superior, añade. «Este último producto ya está listo, pero no se ha lanzado al mercado porque se están definiendo los términos de su comercialización. Por el momento, los usuarios pueden descargar la aplicación desde nuestro sitio web».

Otras prestaciones, como las consultorías remotas, la configuración segura de los proxys o el hackeo ético para comprobar el nivel de seguridad de los servidores, sí son exclusivas para las empresas.

Al decir de la directora de Segurmática, las afectaciones más frecuentes en el escenario nacional son los llamados ransomware (programas que encriptan información), y aunque todavía hay virus que entran a las PC mediante los puertos USB, lo más usual es que lleguen a través de correos electrónicos o en el acceso a páginas web.

«Para conocer estos datos, nos retroalimentamos con las muestras y reportes que envían los clientes y que analizamos en nuestro laboratorio, además de que monitoreamos el tráfico de Internet que circula por Cuba. Estas acciones nos

permiten detectar aplicaciones malignas e incorporar la solución en nuestro antivirus».

Gonzalo García Pierrat puntualiza que el troyano es otro de los programas malignos que más afecta a las redes institucionales.

Este tipo de hack controla a la computadora. El atacante puede estar a miles de kilómetros de distancia, y sin embargo, podrá leer, borrar o mover cualquier archivo, además de enviar todo el tráfico de datos que desee desde esa dirección IP, explica.

«Estos programas se introducen a través de las vulnerabilidades del sistema operativo instalado. Las redes informáticas son complejas, brindan una gama alta de servicios y aplicaciones, y si estos no son bien configurados, aparecen entonces las brechas».

De ahí que uno de los objetivos de la OSRI sea verificar cuál es el origen del fallo y alertar de la situación a la entidad afectada.

«Antes de que un usuario entre a la red nacional y detecte las vulnerabilidades, nosotros hacemos ese trabajo de rastreo. Y los clientes lo agradecen, porque es preferible que nosotros le señalemos las fisuras, a que alguien —desde afuera o dentro del país— ataque su sistema de telecomunicación».

Lo otro, menciona García, es tratar de hacer un trabajo proactivo a partir de divulgaciones, talleres y conferencias. «Asimismo, realizamos controles a las empresas y organismos estatales, lo cual nos permite conocer cómo se aplica en la práctica la base legal y las regulaciones emitidas por el Mincom. Así, también vamos creando una cultura, un conocimiento sobre seguridad informática, que tanta falta hace».

¿INFORMATIZADOS O SEGUROS?

Estamos en un momento de oportunidad, de apropiarnos del desarrollo y recuperar la capacidad de las organizaciones de servir, basadas en las relaciones digitales. Para ello, hay que seguir insistiendo en la formación informacional e incentivar las posibilidades de acceso a las TIC, comenta a Granma Yarina Amoroso.

«Lo más representativo no es el empleo de la tecnología en sí, sino la posibilidad de abrir canales de comunicación cada día más directos para acercar a autoridades, instituciones y ciudadanos. Gestionar información, servirnos de esos sistemas e interactuar como ciudadanos en red hacen parte del presente».

En este sentido, seguridad e informatización no pueden ir por caminos separados. No podemos pretender dar el salto hacia una cultura digital –amen de toda la infraestructura, despliegue de la industria del software y respaldo económico que se necesita– si no tenemos en cuenta que en la medida en que las TIC formen parte cotidiana de los servicios y cadenas de producción del país, tal accionar deberá ir acompañado por una cultura y protección de la información.

Poco obraríamos en el propósito de transformar la sociedad, si cuando el cliente llega a la oficina comercial no puede gestionar su compra por dificultades técnicas que pudieron ser previstas, o tiene que desplazarse hacia otro cajero automático porque el más cercano estaba fuera de servicio. La disponibilidad del recurso y la capacidad de la red para recuperarse rápidamente ante cualquier fallo, dependen también de ese complejo entramado que es la seguridad informática.

Por otra parte, el acceso a Internet, bases de datos nacionales y registros de instituciones públicas, tiene que ir a la par de una estrategia de ciberseguridad que, sin convertirse en enemiga del desarrollo, pueda regular adecuadamente los derechos y deberes de los ciudadanos en el uso de los medios de informatización, a la vez que haga frente a los delitos y asegure la soberanía tecnológica.

El reto: estar informatizados y seguros.

[:]