Experiencia cubana en la protección contra los virus informáticos

José Bidot Peláez
Director de CEDISATEMA. Presidente de la Comisión Nacional de Protección de Datos de Cuba

Por su analogía con los virus biológicos, se les llama virus informáticos, a programas escritos por especialistas de computación que se reproducen a sí mismos y además ejecutan una acción o efecto secundario en los sistemas que infectan, pero a diferencia de los virus biológicos, desgraciadamente, los virus informáticos son resultado del trabajo mal orientado del hombre, no de la obra de la naturaleza.

Los virus atentan contra la productividad del trabajo de las computadoras ya que afectan sus recursos principales: el tiempo de procesamiento y el espacio de memoria disponible del Sistema; tanto la memoria operativa (RAM), como la memoria externa de los Discos Duros y disquetes, y pueden ser capaces de alterar, destruir o borrar la información contenida en las computadoras, mutilando en segundos el esfuerzo de especialistas de meses o tal vez años, con la consecuente pérdida de recursos materiales y humanos.

El desarrollo creciente de las aplicaciones de la informática en nuestro país ha incrementado su dependencia a los sistemas automatizados, los cuales se ven amenazador por la acción devastadora de los virus informáticos, que pueden poner en peligro actividades tan importantes como la salud (fundamentalmente en relación con el diagnóstico clínico), las investigaciones científicas, los controles económicos y financieros, la automatización industrial, los servicios de reservación de pasajes, hoteles y otras capacidades, el pago de la seguridad social, el cobro de servicios como el telefónico, la electricidad, el gas, además de otros que harían muy extensa esta relación; lo que causaría cuantiosos daños económicos y sociales.

Revista General de Información y Documentación, Vol. 4 (2), 221-226, Editorial Complutense, Madrid, 1994

Teniendo en cuenta que en el mes de julio de 1989 se registraban 15 virus y que el año 1993 comenzó con más de 2400, el incremento internacional de los mismos sigue un comportamiento exponencial y seguirá aumentando alarmantemente en los próximos meses, por lo que debemos prepararnos para trabajar teniendo en cuenta la existencia permanente y creciente de los virus, lo que nos obliga a perfeccionar nuestros sistemas de protección y a incrementar el nivel de conocimientos de los usuarios y especialistas de la Informática ante este nuevo tipo de riesgo de la aplicación de las técnicas de computación.

LA EXPERIENCIA CUBANA

En marzo de 1988, se detectó en nuestro país, la presencia del virus conocido como Vienna 648, el cual desató una epidemia que se extendió por toda la isla, demostrando lo vulnerable que eran nuestros sistemas.

A partir de esa amarga experiencia la Comisión Nacional de Informática designó a un miembro de su ejecutivo, para presidir la Comisión Nacional de protección de datos, a la cual asignó entre sus funciones, trabajar de forma inmediata en lo relacionado con la protección contra los virus informáticos.

La comisión se integró por especialistas de diversas instituciones del país, los cuales de forma emergente se iniciaron en el trabajo de Protección y Seguridad de los datos que se procesan en medios técnicos de computación.

Así, desarrollando un trabajo colectivo y de intercambio de experiencias y conocimientos, se dirigió el esfuerzo inicial a lograr los siguientes objetivos:

— Recopilar información técnica internacional relativa a los virus informáticos.

— Ampliar los conocimientos sobre los llamados programas «asesinos», fundamentalmente en relación con los virus.

— Estudiar detalladamente el código de los dos primeros virus detectados en el país: el virus VIENNA 648 y del virus ITALIAN (alias BOUNCING BALL), infectores de programas y boot sector, respectivamente.

— Dominar los productos utilitarios de SOFTWARE necesarios para trabajar en la detección, aislamiento e investigación de los virus.

— Estudiar productos antivirus de SOFTWARE fundamentalmente del tipo SCANER para la identificación de los virus que fueran apareciendo en el país.

— Adiestrar de forma acelerada a los especialistas en cuanto a detectar, aislar e investigar los nuevos virus que fueran detectándose en el País.

— Elaborar un conjunto de medidas técnico-organizativas de rápida implementación por parte de las entidades utilizadoras de las técnicas de

computación que permitieran prevenir, detectar y minimizar la acción de los virus, además de la descontaminación de sistemas infectados.

Una vez logrados los objetivos iniciales la Comisión orientó su trabajo a:

1. Establecer un Sistema Unico Nacional para reportar a la Comisión la presencia de cada «nuevo» virus de computadoras que apareciera en el país, y posteriormente informar a los especialistas y usuarios nacionales sobre su descripción, clasificación, síntomas y daños potenciales que ocasionaran, además de los productos de software antivirus que pudieran utilizarse para contrarrestar su acción.
2. Crear una cultura de protección informática en los directivos, técnicos y usuarios de las técnicas de computación, y en los estudiantes de los diferentes niveles del sistema de educación nacional donde se imparten conocimientos sobre estas técnicas.
3. Investigar técnicamente los virus que se detectan en el país y establecer sus orígenes, así como al desarrollo de productos de SOFTWARE ANTIVIRUS para contrarrestar su acción.
4. Crear un Fondo de Programas de Software Antivirus y de protección a partir del desarrollo nacional, cuyos productos se actualizan cada vez que un nuevo virus es detectado en el país.
5. Estudiar las condiciones que rigen en el país para proponer soluciones jurídicas que correspondan con el nivel de desarrollo actual y perspectivo de la Informática en Cuba y la integridad, seguridad y uso adecuado de los datos que se procesan en medios técnicos de computación.
6. Implementar un Sistema de Protección contra los Virus Informáticos en los eventos nacionales e internacionales celebrados en nuestro país donde intervienen medios técnicos de computación.

Los primeros virus que detectamos causaron epidemias que infectaron sistemas a lo largo del país, sin embargo el trabajo sistemático de la Comisión y de los responsables de la Protección de Datos de los organismos nacionales, ha permitido reducir significativamente los daños que potencialmente los 31 virus detectados hasta la fecha en el país pudieron ocasionar, teniendo en cuenta que algunos de estos virus pudimos «aislarlos» en los primeros Sistemas que afectaron, por lo que no pudieron dispersarse por el territorio nacional y en otros casos los neutralizamos antes de que ejecutaran su fase de «acción».

DESARROLLO NACIONAL DE PRODUCTOS ANTIVIRUS

Desde su constitución la Comisión Nacional ha dedicado gran parte de sus esfuerzos al desarrollo nacional de productos de SOFTWARE ANTIVIRUS, política que actualmente reafirmamos, teniendo en cuenta el comportamiento internacional del incremento de los virus según las siguientes estadísticas.

— Más de cuarenta países se encuentran registrados como productores de Virus (siendo los tres primeros en encabezar este índice negativo los Estados Unidos, Bulgaria y Rusia).

— Como promedio durante el año 1992 aparecieron en el mundo más de 4 nuevos virus diariamente.

— En nuestro país se han detectado 35, lo que representa el 1,4 por 100 de los registrados internacionalmente.

La práctica nos demuestra que la lucha no debe librarse contra «TODOS» los virus existentes Internacionalmente, sino contra los virus existentes, o mejor aún, contra los virus prevalecientes en el país.

Atendiendo al incremento promedio de los virus, los productos antivirus del tipo identificadores o SCANER, «envejecen» a diario y ha sucedido que aunque se cuenta con productos que identifican a miles de virus, no así a algunos de los 36 detectados en el país, por lo que al utilizarlos nos obligan a preguntar irracionalmente por miles de virus que no han aparecido en el país y sin embargo resultan insuficientes con relación a los 36 detectados.

Esta realidad nos obliga a trabajar en la investigación y desarrollo de productos nacionales de software antivirus, que podamos actualizar ágilmente cada vez que un «nuevo» virus es detectado en el territorio nacional, considerando además, que los virus nacionales no serían identificados por los productos extranjeros y hasta la fecha hemos registrado 4 que representa el 11 por 100 de los detectados en el país.

INFORMATICA'94

2.º Seminario Iberoamericano de protección contra los virus informáticos

Durante la realización de Informática'90: la Comisión, para garantizar la salud informática de expositores y participantes, realizó un control a los soportes magnéticos que intervinieron en el evento, detectando 120 disquetes y 11 Discos Duros contaminados. El control permitió detectar, en Pabellones de expositores extranjeros, los virus DISK KILLER y VACSINA, los cuales no habían aparecido anteriormente en el país, lo que nos permitió «aislarlos» y desarrollar los correspondientes productos recuperadores y descontaminadores para ellos.

Esta experiencia se repitió durante Informática'92, detectando en esta ocasión 85 disquetes y 23 Discos Duros infectados por 9 virus, encabezados por el entonces célebre Michelangelo.

Como parte de la Convención Informática'94, respondiendo a la importancia que Cuba concede a la lucha contra los virus, organizaremos el «2.º Seminario Iberoamericano de protección contra los Virus Informáticos» el cual dará continuidad al evento celebrado durante la edición del 92, primero de su tipo en la Región.

El seminario tiene como objetivos principales la presentación de ponencias sobre la situación internacional que presentan los virus, el desarrollo de SOFTWARE ANTIVIRUS, las experiencias legales y las políticas desarrolladas para combatir los virus informáticos.

Además, Cuba mostrará los resultados alcanzados por la Comisión y los servicios informáticos que en esta especialidad puede brindar a entidades de otros países que lo soliciten, como por ejemplo:

— Servicios de detección y descontaminación in situ.
— Desarrollo de productos de SOFTWARE ANTIVIRUS adecuAdos a los virus prevalecientes o detectados en el país que solicite el servicio.
— Asesoría técnica.
— Cursos y entrenamientos prácticos de:
  • Protección contra virus informáticos.
  • Uso efectivo del software antivirus.
  • Técnicas para el aislamiento e investigación de virus.
  • Recuperación de datos en discos.
  • Aspectos jurídicos a considerar en la lucha contra los virus.

UN LABORATORIO LATINOAMERICANO

Como reconocimiento al trabajo desarrollado por los especialistas cubanos el Programa Intergubernamental de Informática (PII) de la UNESCO aprobó la creación en La Habana del Laboratorio Latinoamericano para la Protección contra los virus informáticos, el cual tiene entre sus objetivos principales trasmitir los resultados y experiencias de Cuba a otros países de la región.

El Laboratorio sirve como Centro coordinador para reportar la presencia de nuevos virus en los países miembros y pone a disposición de éstos, Bases de datos con información sobre las características, síntomas y daños que pueden ocasionar los virus detectados en la Región y en el Mundo.

Además trabaja en el aislamiento, estudio e investigación de los virus reportados y en el desarrollo de productos de software antivirus los cuales forman parte de un fondo de programas para contrarrestar la acción de los virus en la Región.

El laboratorio contribuye a la capacitación de docentes e investigadores para que a su vez puedan capacitar a especialistas de sus respectivos países, y propicia el intercambio de experiencias legales y jurídicas en este campo, Así como en lo relacionado a las políticas y estrategias para desarrollar la lucha contra los virus.

Los especialistas del Laboratorio brindan servicios de detección y descontaminación in situ, asesoría técnica, cursos y entrenamientos en los países que lo soliciten, experiencia que ya se ha practicado con éxito en coordinación con instituciones docentes de México.

UN CONSEJO

Temiendo en cuenta la cantidad de microcomputadoras existentes en el mundo, que trabajan con el Sistema Operativo MS-DOS y el intercambio y comercialización despiadado de códigos de virus, se pronostica que la cifra de más de 2400 virus con que comenzó el año 1993 se multiplique en los próximos años, por lo que debemos prepararnos a «convivir» con los virus informáticos, así que no se demore, contáctenos...