DOMPDF_ENABLE_REMOTE is set to FALSE
file:///var/www/html/portal_mincom_v2/sites/all/themes/mincom/logo.png
Ministerio de Comunicaciones
Published on *Ministerio de Comunicaciones* (https://www.mincom.gob.cu)

DOMPDF_ENABLE_REMOTE is set to FALSE
file:///var/www/html/portal_mincom_v2/sites/default/files/styles/noticias/public/ciberseguridad_0.jpeg

Hablando de ciberseguridad (I)

Fuente:
Tomado de Cubadebate, Omar Pérez Salomón

Uno de los temas que más debate y polémica suscita hoy a nivel internacional es la ciberseguridad, por su impacto en el orden económico, político e ideológico y de la seguridad de las naciones. Sobre este importante asunto estaremos conversando en varios trabajos con Miguel Gutiérrez Rodríguez, Director General de Informática del Ministerio de Comunicaciones de Cuba, experto en sistemas informáticos y ciberseguridad.

OPS: Miguel, usted fue nombrado recientemente Director General de Informática del Ministerio de Comunicaciones (MINCOM); antes, fungió como Vicepresidente de Tecnologías en las empresas de Correos de Cuba y la de Desarrollo de Software (Desoft), y Director de la Oficina de Seguridad para las Redes Informáticas (OSRI) de nuestro país por espacio de cinco años. ¿A partir de su experiencia en qué contexto Cuba está adoptando un grupo de medidas para proteger de manera efectiva su ciberespacio nacional?

MGR: El avance en el desarrollo de las Tecnologías de la Información y la Comunicación (TIC) y su influencia en prácticamente todas las esferas de la vida económica, política y social, propició la aparición de comportamientos ilícitos, dirigidos contra las redes y sistemas informáticos, como pudieran ser ataques a servidores, desfiguración de sitios web, denegación de servicios, introducción de códigos maliciosos y envío masivo de correo no deseado (spam), por citar algunos ejemplos, y aquellos que utilizan las redes y sistemas como medio para cometer ilegalidades, tales como el fraude, robo, espionaje, pornografía infantil, entre otros.

En este contexto, en el paquete de normas jurídicas que se deben aprobar para implementar la política de informatización de la sociedad cubana, está un Decreto que establece el marco legal reglamentario que regule y ordene el empleo seguro de las TIC para la informatización de la sociedad y la defensa del ciberespacio nacional, en correspondencia con lo establecido en la Constitución de nuestro país, recientemente aprobada, otras normas legales aprobadas sobre el tema, así como los tratados y demás instrumentos jurídicos internacionales en esta materia, de los que Cuba es Estado parte.

También el Consejo de Ministros aprobó el sistema de trabajo y las medidas para la protección del ciberespacio nacional, que permitirá actuar de forma proactiva en la informatización segura de la sociedad, minimizando los riesgos inherentes a este proceso, organizando la solución de los incidentes de ciberseguridad y la correspondiente mitigación de su impacto negativo.

OPS: ¿Cuándo aparecen los primeros incidentes de seguridad?

MGR: Los incidentes de seguridad en los sistemas informáticos aparecen desde que comenzó el uso de estas tecnologías. En 1947, los creadores de la computadora electromecánica Mark II informaron del primer caso de error en un ordenador causado por un insecto. El equipo sufrió un fallo en un relé electromagnético y durante la investigación se encontró una polilla que provocó que ese relé quedase abierto. Una de las programadoras al registrar el incidente en la bitácora habilitada pegó en ella el insecto con cinta adhesiva y se refirió al él como un bug (bicho) para describir la causa del problema.

OPS: El reemplazo de las válvulas electrónicas por el transistor bipolar y la integración a gran escala de los procesos en pequeños chip de silicio permitieron disminuir el tamaño de los equipos, aumentar su potencia y la capacidad de procesamiento de datos, así como disminuir los precios de los mismos. ¿Qué repercusión tuvo estos adelantos en la seguridad informática?

MGR: Esta evolución tecnológica, positiva por supuesto, trajo consigo que se incrementaran considerablemente los sitios donde los datos y el hardware estuvieran expuestos a diversas amenazas.

A partir de ese momento se comenzó a interconectar las computadoras para compartir datos, formando redes de diferentes tipos y dimensiones en las entidades. A inicios de 1990 estas redes comenzaron a conectarse con otras y surgieron una gran variedad de dispositivos de acceso portátil e inalámbrico. De esta manera se introdujo nuevos factores de riesgo, posibilitando una vía para potenciales accesos no autorizados.

OPS: ¿Cuál se considera el primer ataque a la infraestructura computacional de Internet?

MGR: A finales de 1988 se estimaba que estaban conectadas a Internet unas 60 mil computadoras. El 2 de noviembre de ese año un programa informático atacó la red y afectó durante horas cerca del 10% de todos los ordenadores ubicados en los Estados Unidos, incluyendo los del Centro de Investigación de la NASA. El autor fue Robert Tappan Morris, estudiante estadounidense de 23 años. A ese programa malicioso se le denominó “gusano Morris” (Morris worm) y se considera el primer ejemplo de software malicioso (malware) que afectó a Internet.

OPS: Creo que el juicio a Morris derivó en la primera condena por la ley de fraudes informáticos de 1986 en los Estados Unidos.

MGR: Así es. Morris fue procesado y en el juicio realizado en enero de 1990 la fiscalía argumentó que se trató de un ataque contra el gobierno de los Estados Unidos y el jurado federal lo declaró culpable. De nada valió que los abogados de Morris aseguraran que intentaba ayudar a la seguridad de Internet.