ciberseguridad

Source:
Tomado de La pupila insomne, por Omar Pérez Salomón

Cuando se trata de la seguridad de las Tecnologías de la Información y la Comunicación, es muy frecuente en las entidades y organismos, que se le preste mayor atención al establecimiento de controles de tipo administrativo y técnico, y muy poca al modo de actuación ante un incidente de ciberseguridad. Esto trae como consecuencia, que en situaciones críticas se tomen decisiones apresuradas o que no son las más idóneas y podrían conducir a la pérdida de información importante para los procesos investigativos a realizar para el esclarecimiento de los hechos. Sobre esta importante cuestión estaremos hablando con Miguel Gutiérrez Rodríguez, Director General de Informática del Ministerio de Comunicaciones de Cuba.

– Miguel, ¿qué características tuvieron los incidentes que afectaron los sistemas informáticos cubanos en el año 2019?

– En general, hubo una disminución de los incidentes en el año 2019 en relación con el 2018, también fueron menos las reclamaciones internacionales enviadas desde nuestro país y las recibidas desde otros paises. Los virus informáticos incrementaron su posición respecto a los incidentes ocurridos en 2018, registrándose un incremento de la actividad de programas malignos, en particular la categoría “caballo de Troya” en un 18.84% de la ocurrencia total. La actividad de correo no deseado (Spam) registró un 12.95% de ocurrencia.

Las categorías principales de incidentes ocurridas el año anterior fueron los programas malignos, acciones no autorizadas sobre los sistemas, correos no deseados, afectación de los sistemas, denegación de servicio y desfiguración de sitios web. En el segundo semestre de 2019 el comportamiento fue el siguiente:

– ¿Cuáles son las reglas a seguir para minimizar la cantidad y repercusión de los incidentes de ciberseguridad?

– La preparación para afrontar incidentes es vital si queremos reducir su impacto nocivo. En este sentido es preciso definir con antelación una estrategia de respuesta a los mismos y tener en cuenta un grupo de reglas para lograr ese propósito. Entre ellas tenemos:

Ø Establecer y poner en práctica políticas y procedimientos para la gestión de incidentes.

Ø Evaluar de forma sistemática las vulnerabilidades del entorno.

Ø Comprobar con regularidad todos los sistemas y dispositivos de red para garantizar que tienen instaladas las revisiones más recientes.

Ø Establecer programas de capacitación sobre seguridad.

Ø Supervisar y analizar con regularidad el tráfico de red y el rendimiento del sistema.

Ø Comprobar los procedimientos de restauración y copia de seguridad.

Ø Actualizar los planes de medidas de ciberseguridad

Ø Priorizar las capacidades de supervisión y monitoreo propias.

Ø Perfeccionar las estructuras especializadas en ciberseguridad

– ¿Cuáles son las proyecciones de trabajo del Ministerio de Comunicaciones para este año en lo referido a la

gestión de incidentes?

– Son varias las proyecciones, dentro de ellas tenemos: Crear cultura de ciberseguridad en la poblacion para el uso de las TIC, concluir la fase de aprobación de normas pendientes y capacitar a personas jurídicas y naturales dada la transversalidad de la ciberseguridad; continuar incrementando la protección del ciberespacio nacional; perfeccionar la ciberseguridad en el ámbito tecnológico, incrementar la capacidad de producción de herramientas propias, fomentar el desarrollo de las entidades especializadas; incrementar el control y fiscalización en materia de Ciberseguridad; aplicar la legislación vigente en materia de contravenciones ante conductas violatorias e indisciplinas que generen incidentes ciberneticos o creen las causas y condiciones para su ocurrencia; aprovechar al máximo las posibilidades de la cooperación internacional y fomentar de conjunto con los Organismos de la Administración Central del Estado, la capacitación y concientización de todo el personal y la población en general.