La defensa debe ser **proactiva**

Las tendencias, los retos y las oportunidades de la ciberseguridad y la ciberdefensa fueron analizados en dos foros a cargo de estrategas y consultores internacionales y de empresas públicas y privadas del país.

"La defensa es la labor que le corresponde al Estado. La seguridad nos toca a todos como ciudadanos, empresas o cualquier negocio."

Erick Erez Kreiner, presidente Five C y asesor senior del Israeli National Cyber Bureau.

Esta es una de las diferencias entre estos dos conceptos que marcó Erick Erez Kreiner, presidente Five C y asesor senior del Israeli National Cyber Bureau, al introducir el panel "Tendencias y retos en defensa cibernética". El ciberespacio de un país —explicó— se puede dividir en tres subdominios: las fuerzas del Gobierno y la infraestructura crítica, las empresas y las corporaciones, y el público en general. "Si miramos el ciberespacio encontramos la defensa, y cuando miramos a los subdominios, hallamos la seguridad".

La defensa debe ser proactiva, recalcó. "No podemos modificar las tendencias, si uno navega, no puede cambiar el viento. Eso quiere decir que, si hay amenaza de ataque, tiene que haber tendencias de seguridad o defensa para contrarrestarla. Es necesario estar interceptando y atacando aun dentro de la propia red, pues uno la conoce mejor que el enemigo y sabe dónde puede esperarlo, en un sitio que él no se imaginaría que lo van a asaltar". Para ello, los ejércitos, las armadas, las fuerzas aéreas, emplean armas que utilizan los *hackers* y esta es una tendencia de la tecnología desarrollada en el dominio civil, que pasa al militar y viceversa, agregó el estratega.

"La defensa debe evitar el ataque antes de que suceda, pero si ocurre hay que poder enfrentarlo. Si tiene éxito, debe poder contener el daño y, si lo causó, debe tener la capacidad de recuperarse rápidamente y asegurarse de que no se repita".

Este panel fue moderado por en profesor Nelson Remolina, director del Grupo de Estudios en internet, Comercio electrónico, Telecomunicaciones e Informática (GECTI) de la Universidad de los Andes, quien les preguntó a los participantes sobre qué capacidades de defensa tienen en sus áreas y qué pueden hacer ante un ataque.

> "Hay que transformar el modelo eminentemente reactivo en uno preventivo. Hoy tenemos exceso de información y falta convertirla en conocimiento que permita anticipar la acción".
>
> **Coronel Jairo Gordillo**

El **Coronel Erich Siegert Cerezo,** comandante del Comando Conjunto Cibernético de las Fuerzas Militares (CCOC), señaló que ese organismo es responsable de crear las capacidades para la defensa de un posible ataque en el ciberespacio. Y agregó que, a nivel mundial, el ciberespacio es considerado como un quinto teatro de operaciones del dominio de la guerra y hay que prepararse.

El **Coronel Ernesto García Luna,** director del Centro de Inteligencia Técnica del Ejército (CITEC), dijo que los trabajos en este sentido están evolucionando y se debe compartir la experiencia y la capacitación de los sectores públicos para

fortalecer el Estado. Así mismo, hay que prevenir, disuadir y reaccionar ante un ataque a la infraestructura crítica.

Jeffry R. Mausolf, experto en inteligencia de IBM, anotó que se han mejorado la concientización y la educación, pero ante la gran cantidad de personas con acceso a internet, la inquietud es si ellas y las empresas saben de los riesgos. "No podemos protegerlo todo, pero hay que identificar las prioridades y conocer nuestros atacantes para estar mejor preparados".

Óscar Arias, coordinador del Grupo de Respuesta a Emergencias Cibernéticas (ColCERT) del Mindefensa, coincidió en que para mejorar la ciberdefensa es necesario coordinar a los grupos existentes, tarea en la que están trabajando. Agregó que es importante precisar cuándo el incidente compromete la seguridad nacional, por lo cual procuran establecer cuáles son las infraestructuras y los activos más críticos del país y cuándo un ataque puede comprometer la seguridad y defensa nacionales para determinar qué tácticas de ciberdefensa o de seguridad deben emplear.

Oscar Guitron, de EMC/RSA, dijo que en seguridad se tienen componentes, procesos, gente y tecnología. En términos de personas se necesita una buena capacitación, estar actualizados sobre las tendencias de ataques, cómo actuar ante ellos, cómo protegerse.

Jeimy José Cano de Ecopetrol, Diego Zuluaga de Isagen, Zohar Elnekave de RSA/EMC, José Montoya de Bancolombia, Daniel Rojas, de Symantec, Sandra Rueda de Uniandes, Jorge Bejarano de MinTIC y la moderadora del panel, Mónica Parada, de *La República*.

Añadió que en RSA identificaron cuatro características de la tecnología para que sea útil en el combate de los ataques. Entre ellas está que ofrezca visibilidad de lo que está ocurriendo de afuera hacia adentro y en la compañía.

Otra característica son los APT, (*Advanced Packaging Tool*), un tipo de ataque con el que tratan de permanecer invisibles dentro de la red, para obtener información y extraerla. Por eso es importante esa visibilidad y experiencia y tener expertos analíticos para identificar tendencias en la actividad anormal en la red.

Y en términos de procesos, hay que estar preparados porque nos van a atacar, tener procedimientos definidos para que cuando llegue ese instante sepamos qué hacer. También es necesario definir mecanismos de colaboración con otras instituciones que tengan información importante.

El **Coronel Jairo Gordillo Rojas,** jefe de la Oficina de Telemática Policía Nacional (CSIRT-PONAL), señaló la importancia de aprovechar los esfuerzos del país y articular los procesos para que esta información fluya. Hay que transformar el modelo eminentemente reactivo en uno preventivo. Hoy tenemos exceso de información y falta convertirla en conocimiento que permita anticipar la acción.

Sobre cómo mejorar las capacidades de ciberdefensa, **Juan Diego Jiménez**, coordinador de Infraestructura Tecnológica del Departamento de Ingeniería de Sistemas y Computación (DISC) de Los Andes, expresó que lo resumiría en tres elementos: formación, especialización y coordinación.

"En el primero, si no empleamos la capacitación de manera adecuada, probablemente vamos a reaccionar pero no seremos proactivos. Se necesita especialización en el sentido de que las personas hagan una carrera y podamos formar un semillero de gente".

Por último, agregó, la coordinación es importante porque ahí podemos adquirir capacidades para dar respuesta y predecir los ataques.

Las infraestructuras críticas

¿Cuáles son los factores clave para cumplir con la misión de proteger las infraestructuras críticas?, preguntó el moderador.

Según el coronel Erich Siegert Cerezo, "desde el año pasado hemos sostenido reuniones de trabajo con más de 60 empresas grandes y venimos trabajando en 10 guías de riesgos para establecer unos protocolos que se aplicarán en caso de sufrir un ataque a una de las infraestructuras críticas".

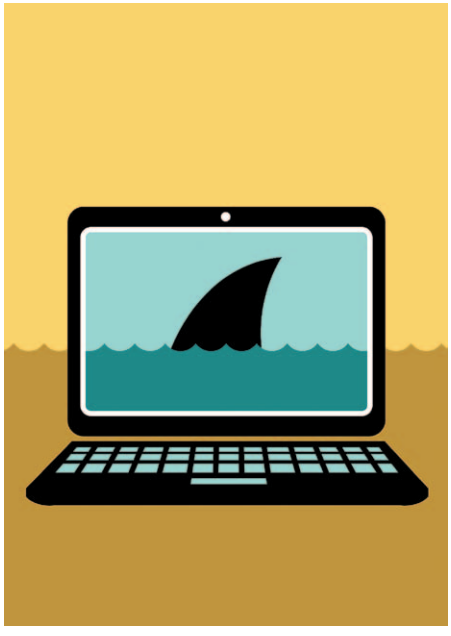

Foto: EFF-Graphics (Trabajo propio) [CC-BY-3.0 (http://creativecommons.org/licenses/by/3.0)], undefined

Hay que identificar las prioridades y conocer nuestros atacantes para estar mejor preparados, dijo Jeffry R. Mausolf.

Todas estas cosas pueden inducir al ciberterrorismo, al ciberespionaje o a la ciberguerra.

CIBERTERRORISMO | CIBERESPIONAJE | CIBERGUERRA

Ciberseguridad:	Ciberdefensa:	Ciberataques:	Cibercrimen:	Ciberarmas:
Aplicación de prácticas de seguridad y control con impacto fuera de la organización. Se basa en monitoreo activo. No se busca prevenir sino identificar y actuar en consecuencia.	Capacidad para defensa activa y contra medidas ofensivas. No se busca detener al atacante sino confundirlo, caracterizarlo y combatirlo.	Acciones no autorizadas realizadas en un sistema informático que comprometen la confidencialidad, la integridad y la disponibilidad del objeto o de la información allí residente.	Manifestaciones de conductas punibles en el contexto del ciberespacio. Actos motivados con intención de daño, bien sea en el contexto, físico, lógico o de contenidos.	Un dispositivo o conjunto de instrucciones informáticas destinadas a dañar ilegalmente aspectos específicos de un sistema que actúa como una infraestructura crítica.

Cuadro presentado por Jeimy José Cano.

"En principio hemos definido 21 sectores, de los que seleccionamos subsectores que van a ser parte crítica y así buscamos que el Comando Conjunto Cibernético esté asegurando el sector defensa y trabajando para el país", agregó el coronel. Estas reuniones buscan lograr una coordinación permanente a través de canales estructurados directos donde se intercambie información de posibles amenazas o ataques en el ciberespacio.

Los datos, los que más peligran

"El 2012 fue el año de las megafugas de datos y se comprometieron cerca de 500 millones de ellos en el mundo", informó Daniel Rojas, de Symantec, en el panel sobre seguridad, en el que participantes de los sectores energético, financiero, académico y seguridad informática coincidieron en que la información es la que más atacan los ciberdelincuentes.

Por eso señalaron en que hay que fortalecer la capacidad de reacción y prevención.

Zohar Elnekave, consultor de RSA, División de Seguridad de EMC, destacó que las amenazas son muy sofisticadas y los *hackeo*s no van a parar. Las empresas deben ser proactivas lo que implica tener visibilidad total de qué pasa en su su red en tiempo real.

La tendencia en el mundo, agregó, es que solo con una inteligencia compartida y con la colaboración entre organizaciones y el Gobierno, se puede combatir eficientemente el ciberdelito.

Mónica Parada, del diario *La República* y moderadora del panel, interrogó a los participantes sobre los riesgos qué afrontan las industrias. Estas fueron algunas respuestas:

Diego Zuluaga, Isagen

Hace cuatro años trabajamos en las guías de ciberseguridad en el sector eléctrico, un área base para el desarrollo económico y el estilo de vida actual. Es un sector interconectado y la falla en uno de sus agentes puede afectar a todo el país, puede, incluso, haber un apagón nacional por medios electrónicos.

Zohar Elnekave, RSA-EMC

Colombia ha mejorado especialmente en el sector bancario. Sin embargo, la seguridad cibernética debe ser proactiva y todavía es reactiva. Una ventaja es que las amenazas nos llegan tarde y las organizaciones pueden aprender de esa experiencia.

José Montoya, Bancolombia

En Latinoamérica, el 40 % de las personas reúsan hacer transacciones electrónicas por miedo a ser defraudadas. Es importante tener un balance entre la seguridad y la usabilidad. Antes los delincuentes iban tras el robo de dinero, ahora van por la información.

Daniel Rojas, Symantec

La información es lo que más buscan. Entre 2012-2013 los ataques dirigidos, en los que está perfilada la víctima, crecieron en el 91 %. Y en el periodo anterior aumentaron en un 42 %, lo cual ya era alarmante. Buscan la información porque les permite cometer fraudes a gran escala.

Sandra Rueda, profesora Uniandes

En Colombia, las empresas pequeñas y medianas están empezando a despertar a esos riesgos, pero carecen de presupuestos y de preparación para enfrentar la situación. Hay información en inglés pero no hablan ese idioma.

Jorge Fernando Bejarano, director de Estándares y Arquitectura de TI del Ministerio TIC

Llevamos años trabajando en estos temas y en Gobierno en Línea para que los ciudadanos puedan interactuar con confianza. Nos ocupan las amenazas que afectan la calidad del servicio y las que buscan robar datos porque el *hacktivismo* está atacando las entidades públicas. Otro peligro es que se use la infraestructura del Estado para cometer ciberdelito. ■

Ecopetrol - Jeimy José Cano

El contexto físico del ciberespacio se conoce —la plataforma tecnológica y de comunicaciones, el software y los servicios—, mientras que el ciberespacio es atemporal, ubicuo, permeable, fluido, participativo, multiidentidades, autorregulado.

Actualmente hay amenazas y riesgos latentes que están en el entorno, pero las organizaciones no conocen qué son el ciberterrorismo, el ciberespionaje, la ciberarma y las amenazas con ciberarmas.

Las otras las conoce la organización, como los ciberataques que son focalizados, el ciberactivismo y el sabotaje a los sistemas de control.

Eso implica varios retos porque el concepto de inteligencia no es el que desarrollan los militares pues el escenario ya es distinto; hay que definir las posturas defensivas y caracterizar los ciberataques para establecer mecanismos de defensa a nivel internacional.