Prácticas de Seguridad de la Información: Reflexiones en la Web 2.0

Jeimy J. Cano, Ph.D, CFE

En este espacio se muestran algunas de las inquietudes de mayor interés sobre ese ambiente.

Uno de los aspectos que despierta gran preocupación en torno al avance de la Web 2.0, es la seguridad, en todas sus dimensiones. Bien sabido es que las redes sociales, entre las alternativas que rodean esas nuevas tecnologías, además de acercar a los seres humanos, ubicados a lo largo y ancho del mundo, también han generado todo tipo de actos delictivos. Hechos que mantienen a las autoridades de los distintos países en vilo, toda vez que la regulación, en la mayoría de los casos, se queda corta.

De ahí que los usuarios tengan que ser creativos para generar distintos mecanismos para protegerse y velar por su información.

A continuación algunas de las inquietudes que frecuentemente se formulan sobre la seguridad dentro de ese

contexto, que despiertan mayor interés, y algunas sugerencias y comentarios al respecto.

¿Cómo define la seguridad frente a la penetración de la web 2.0 en la sociedad?

Cada vez más, la seguridad de la información se acerca a las personas, a sus hábitos, sus comportamientos y valores con relación al manejo de la misma. La seguridad en un entorno como la Web 2.0 es una propiedad personalizada, que siguiendo unos parámetros generales y buenas prácticas, tiene sentido para aquel que lo maneja y exige de ésta resultados diferentes. La Web 2.0 fue pensada para un mundo instantáneo, para una realidad cambiante y un usuario en permanente movimiento.

Así las cosas, la seguridad de la información en ese escenario debe ser una práctica general de aseguramiento de dispositivos y servicios, ajustada a la realidad del usuario que hace uso de ella.

¿Cómo está Colombia en ese tema?

La Web 2.0 tiene un alto grado de penetración en el país, más por sus posibilidades y alcances, desde el punto de vista comercial y personal, que por las consideraciones de seguridad y control que se requieren.

Recientemente, se han revelado noticias sobre el uso de las redes sociales para materializar conductas criminales que han acabado con la vida de adolescentes y personas que con frecuencia interactúan a través de estos medios.

Las redes sociales son un gran medio para compartir e intercambiar con los amigos y grupos de interés, pero mal utilizadas o configuradas de manera inadecuada, pueden ser fuente de información personal sensible que puede afectar el buen nombre o la integridad de las personas, con desenlaces inesperados.

En su opinión ¿cuáles son los mayores riesgos?

Los riesgos de la Web 2.0 están asociados con el aprovechamiento de todas las utilidades de esta realidad, como lo afirma McAfee en su reporte Global threat Intelligence: *"(...) virtually all types of online content from videos to blogs, online articles to annual reports, presents an opportunity for malware to propagate and infect systems and networks*". (http://secure.nai.com/us/mcafee_labs/gti.html)

En tal sentido, las prácticas de seguridad y la administración de riesgos que cada persona adelante frente a su realidad en la Web 2.0, será parte esencial de los mecanismos de autoprotección y aseguramiento que cada persona desarrolle frente al manejo de su información y los dispositivos que utilice para su acceso en línea.

¿Qué tipo de mecanismos los pueden controlar?

Los mecanismos de control para las amenazas en la Web 2.0 empiezan y terminan con las personas, su apetito frente al riesgo y la generación a la que pertenecen.

Esto es, considerar con claridad el tipo de información que se comparte, los alcances de la misma en la activación de aplicaciones o funciones adicionales de las plataformas disponibles, y las necesidades propias de los nacidos entre 1980 y 1990, quienes hoy por hoy están al frente de las tendencias móviles y de conectividad 7x24.

De tal manera, los controles más que tecnológicos (los cuales no podrán faltar y se deben configurar) tienen que ver con los aspectos de cultura en la protección de la información; esos son los que harán la diferencia.

Es importante anotar, que entre más se avance en el tiempo, mayor será la necesidad de compartir información, lo que indefectiblemente nos llevará a una pérdida gradual de privacidad, de lo cual todos debemos estar conscientes.

¿En el país se ha desarrollado una cultura al respecto?

Creo que es inminente iniciar el desarrollo de una cultura de autoprotección de la información desde los grados en la primaria y secundaria, que nos permita alinear las necesidades de los nacidos en los 80´s, 90´s y siguientes, con los retos y amenazas que nos muestran los criminales en el internet.

Con la evolución de las tendencias hacia los servicios tercerizados, acceso por demanda a los recursos y distribución de las capacidades tecnológicas de las empresas, es necesario animar a los colegios y universidades a profundizar en el conocimiento y las prácticas confiables, para una adecuada convivencia en internet.

Así mismo, que en el uso de las tecnologías de información y las comunicaciones, la seguridad de la información sea una competencia transversal y requerida, para asegurar no sólo la información personal, sino para desarrollar un hábito que hace parte de la red extendida de seguridad, donde cada individuo hace parte del perímetro de contención y aseguramiento de la información.

Sobre este tema podemos consultar los diferentes documentos disponibles en el Instituto Nacional de Tecnologías de Información – INTECO, de España: http://cert.inteco.es/Proteccion/Menores_protegidos/Para_padres_y_educadores/

En su concepto ¿cuál es la entidad más adecuada para adelantar campañas en ese sentido?

Considero que el tema es de educación y por lo tanto, el Ministerio de Educación, en conjunto con el Ministerio de Tecnologías de Información y Comunicaciones, deben adelantar una estrategia coordinada para que, a la luz de un lineamiento general de buenas prácticas de seguridad y control en la Web 2.0 y, en general en Internet, se canalicen las acciones tanto en los colegios como en las instituciones de educación superior.

Una materia que se podría denominar "Cátedra Internet Seguro", donde se ilustren acciones pedagógicas y prácticas que, en el lenguaje particular de los adolescentes, se convierta en una didáctica que termine en una práctica sistemática e interiorizada, que rinda sus frutos frente a la lucha contra la criminalidad informática en internet: hacerle la vida más difícil al delincuente.

"Es importante anotar, que entre más se avance en el tiempo, mayor será la necesidad de compartir información..."

¿En qué forma los colegios también deben participar?

Una vez exista el lineamiento general del Ministerio de Educación, se debe revisar el currículo académico para que la "Cátedra de Internet Seguro", sea una realidad dentro de la formación de los niños y adolescentes. Esto sin perjuicio, de que cada colegio por iniciativa propia, pueda iniciar acciones en tal sentido.

"La Web 2.0 fue pensada para un mundo instantáneo, para una realidad cambiante y un usuario en permanente movimiento."

De acuerdo con su experiencia en estos temas, ¿cuál es la población más vulnerable?

No hay duda que los niños y adolescentes entre los 7 y los 15 años, etapa donde se revelan a los muchachos nuevas realidades y se advierten importantes cambios hormonales en sus cuerpo. Esta mezcla de química en el cuerpo y el desarrollo de su personalidad y relacionamiento con su entorno, es el caldo de cultivo perfecto para que la delincuencia, a través de un medio tan personal como las redes sociales, Twitter, la mensajería instantánea, entre otros, cautive a estos jóvenes en su período de rebeldía, incitando sus más profundos deseos y retos, para lanzarse sin miedos ni restricciones a cruzar los umbrales que éstos le proponen, con resultados, algunas veces inesperados o dolorosos.

En consecuencia, es necesario hacer un llamado de atención a todos los padres de familia y los educadores para que comprendiendo esta realidad, se adelanten las acciones del caso, encaminadas a hacer de la experiencia de internet, algo verdaderamente emocionante y lleno de cosas positivas y creativas.

Es importante agregar que las personas adultas, con pocos conocimientos de la realidad de la criminalidad en internet, pueden ser también blancos de criminales que, conociendo sus intereses, logren cautivarlos y engañarlos sin que ellos se den cuenta.

Por lo tanto, hay que mantener un mínimo de paranoia bien administrada, para enfrentar el reto de la delincuencia en internet.

Y ¿cuáles los espacios son los preferidos por la ciberdelincuencia?

Los espacios preferidos por los criminales informáticos son aquellos donde el anonimato es la prenda de garantía, el misterio y el riesgo son los motivadores, y la tecnología es el gancho principal para "atrapar" y mantener la atención de las personas que son víctimas de esta realidad.

La ciberdelincuencia conoce con claridad los intereses de los visitantes de internet y saben de sus hábitos (buenos y malos) cuando de interactuar con sus servicios se trata.

En tal medida, todos somos responsables por hacer de nuestra interacción con internet un lugar confiable, educativo e interesante para todos.

Jeimy J. Cano, Ph.D, CFE. *Miembro investigador del Grupo de Estudios en Comercio Electrónico, Telecomunicaciones e Informática (GECTI) de la Facultad de Derecho y Profesor Distinguido de la misma Facultad. Universidad de los Andes. Colombia. Ingeniero y Magíster en Ingeniería de Sistemas y Computación de la Universidad de los Andes. Ph.D in Business Administration de Newport University, CA - USA. Executive Certificate in Leadership and Management del MIT Sloan School of Management, MA-USA, Profesional certificado como Certified Fraud Examiner (CFE) por la Association of Certified Fraud Examiners. Contacto: jjcano@yahoo.com*