Seguridad en el internet

Fuente: SUPERTEL-ECUADOR

Ahora, con el advenimiento de la Sociedad de la Información y con ciudadanos en el mundo cada vez más conectados y globalizados, han aparecido muchos beneficios que hace años podrían haber sido solo un cuento de Julio Verne. Redes sociales, correos electrónicos, comunicación ininterrumpida, son solo pocos ejemplos de lo que podemos advertir.

Este mismo surgimiento tecnológico ha hecho pensar a los proveedores de servicios tradicionales a migrar su oferta a plataformas digitales. Los cambios han sido exagerados y el Ecuador no se ha quedado fuera del contexto. El mejor acceso a "anchura de banda", hizo posible que ahora cerca de 3.4 millones de ecuatorianos estemos conectados a estos servicios.

Como todo progreso, esto tiene sus puntos negativos y muchos han podido encontrar "huecos" o vulnerabilidades para que, mediante estas plataformas tecnológicas, se puedan cometer delitos o fraudes. Esto en el mundo se lo conoce como ciberdelito o algo mejor pronunciado: delitos cibernéticos. Lejos quedó aquel primer gusano que apareció en las redes en donde dentro del código fuente, sus autores pusieron su información confidencial y su intención era la de sol probar las vulnerabilidades de los sistemas. Ahora, los delincuentes han hecho de las suyas y nada se queda fuera de su vista y su desarrollo.

Con la misma velocidad con la que progresa la tecnología, estos "malos genios" de la computación y las redes avanzan. Se estima que los delitos cibernéticos mueven tanto dinero como el narcotráfico o el tráfico de armas, solo que están regados dentro de la red mundial y cada vez con menores oportunidades de hallarlos por parte de las autoridades, para que puedan ser procesados o peor aun, cumplir una sentencia. En el lenguaje común se han usado muchas palabras nuevas para identificarlos: gusano, porque van incrustados en un software para otro fin específico; troyano, porque va escondido como el caballo de Troya, y así podemos definir todos los nombres, la mayoría anglicismos, para una rápida comprensión. Sin embargo, puede encontrar todas las definiciones en una "wikipedia" con una mejor explicación.

Los delitos van más allá de solo robar las contraseñas, ingresar al correo electrónico o a una cuenta de las redes sociales. Por ejemplo, el troyano "torpig" en Europa, se encargó de vaciar cuentas de bancos suizos solo cambiando los campos cuando transmitía fuera del computador del usuario sin que éste lo note. Imaginen en una transacción bancaria en donde el troyano no le importaba sus códigos o contraseñas porque cada uno era directamente ingresado por el usuario, solo interrumpía y cambiaba los datos en la transmisión para que se pueda depositar el dinero en otras cuentas, todo con el aval del dueño que pensaba que estaba haciendo la transacción correcta. Los creadores de tal maravilla fueron localizados en Ucrania, pero no se conoce si fueron o no sometidos por las autoridades.

Con estos antecedentes, varias instituciones en el ámbito mundial han empezado a desarrollar acciones para combate y estudio del ciberdelito. Carnegie Mellon, universidad prestigiosa de Estados Unidos, ha establecido centros de respuestas a Incidentes Informáticos y toda una metodología para implementarlos. De igual manera, la Unión Internacional de Telecomunicaciones – UIT estableció el grupo IMPACT para las acciones en contra de la ciberdelincuencia. Todo esto ha formado frentes de acción y redes de confianza como FIRST, AMPARO; todos los países tienen un Centro de Respuestas conocidos como CERT o CSIRT y son los que investigan o coordinan la investigación de los incidentes.

El Ecuador está proponiendo a través de la Supertel desarrollar el Ecucert para el tratamiento de los incidentes Informáticos. Esperamos que este año, el Ecucert sea una realidad y se empiece a generar capacidades con la academia y con el sector privado para poder realmente desarrollar un gran equipo en este tema en particular. Algo que llama mucho la atención ahora es que en cualquier entidad de seguridad de gobierno ya se pone la ciberdefensa como un tema. Para ejemplo, visiten la página del Departamento de "Homeland Security" de Estados Unidos y verán que hay una sección especial para el tema.

Para concluir, los delitos cibernéticos o ciberdelitos han tenido su aparición desde que los computadores empezaron a poner o procesar información que solo debe ser confidencial para el usuario.

Los servicios y transacciones empezaron a ser cada vez más usados a través de las redes, pero al mismo tiempo aparecieron delitos en estas redes. Por ahora, existen grupos o iniciativas muy bien fundadas para investigación, combate y todo lo relacionado en contra del delito en estas redes. Por eso, la SUPERTEL presenta su revista institucional Nº 13/2012, en donde no solo se habla de temas técnicos, sino que también se trata de generar capacidades en los ciudadanos y en el lector para que la próxima vez que esté en un dispositivo, tenga mayor cuidado y no sea víctima de estas redes que en su mayoría son internacionales.

Fuente: SUPERTEL

Con autorización: Tomado de la revista SUPERTEL No. 13 – **ciberseguridad**