Delitos Informáticos y Terrorismo Computacional

La información constantemente ha sido y será intensamente importante en todo el contexto que se calculen. Imaginemos solamente lo que simboliza un secreto y el valor que tiene para el comprometido y lo que podría significar su descubrimiento para los implicados. Ahora, imaginemos toda la información que está en las bases de datos de las empresas (hospitales, bancos, clubs, hoteles, etc.) Siempre y cuando la información sea utilizada adecuada y legalmente, se puede decir que no hay dificultad. Pero cuando se hace uso indebido, prohibido o ilegal de la misma, incluyendo su acumulación e instalaciones físicas se puede afirmar que se ha incidido en un delito informático. Otro tema significativo y de cuidado es lo referido al terrorismo computacional que es cuando algún equipo de cómputo se convierte en un arma de pánico o terrorismo específicamente.

1. Un delito informático es toda aquella acción, típica, antijurídica y culpable, que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet. Debido a que la informática se mueve más rápido que la legislación, existen conductas criminales por vías informáticas que no pueden considerarse como delito, según la "Teoría del delito", por lo cual se definen como abusos informáticos, y parte de la criminalidad informática.

CARACTERÍSTICAS PRINCIPALES

- Son delitos difíciles de demostrar ya que, en muchos casos, es complicado encontrar las pruebas.
- Son actos que pueden llevarse a cabo de forma rápida y sencilla. En ocasiones estos delitos pueden cometerse en cuestión de segundos, utilizando sólo un equipo informático y sin estar presente físicamente en el lugar de los hechos.
- Los delitos informáticos tienden a proliferar y evolucionar, lo que complica aún más la identificación y persecución de los mismos.

Al parecer de todos los delitos informáticos que ocurren, un porcentaje demasiado alto que supera el 70%, son cometidos por personal de las organizaciones incluyendo el uso indebido de la parte lógica y la parte física de la información. Esto nos indica que es necesario desde un comienzo, concientizar el CEO de una organización para que apoye al CIO en lo referente a realizar una minuciosa selección del personal informático y establecer políticas para escoger muy bien todo el personal contratado, dado que de una u otra forma tendrá acceso a información.

Delitos informáticos:

Fraudes cometidos:

Mediante manipulación de computadoras Estos pueden suceder al interior de Instituciones Bancarias o cualquier empresa en su nómina, ya que la gente de sistemas puede acceder a tos tipo de registros y programas.
La manipulación de programas mediante el uso de programas auxiliares que permitan estar manejando los distintos programas que se tiene en los departamentos de cualquier organización.

Manipulación de los datos de salida Cuando se alteran los datos que salieron como resultado de la ejecución de una operación establecida en un equipo de cómputo.
Fraude efectuado por manipulación informática Accediendo a los programas establecidos en un sistema de información, y manipulando para obtener una ganancia monetaria.

2. LEGISLACION COLOMBIANA CONTRA DELITOS INFORMATICOS:
   La Ley 1273 de 2009 creó nuevos tipos penales relacionados con delitos informáticos y la protección de la información y de los datos con penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes.
   El 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 “Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “De la Protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.

   Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las empresas se blinden jurídicamente para evitar incurrir en alguno de estos tipos penales.

No hay que olvidar que los avances tecnológicos y el empleo de los mismos para apropiarse ilícitamente del patrimonio de terceros a través de clonación de tarjetas bancarias, vulneración y alteración de los sistemas de cómputo para recibir servicios y transferencias electrónicas de fondos mediante manipulación de programas y afectación de los cajeros automáticos, entre otras, son conductas cada vez más usuales en todas partes del mundo. Según estadísticas, durante el 2007 en Colombia las empresas perdieron más de 6.6 billones de pesos a raíz de delitos informáticos.

LEGISLACION DE ESTADOS UNIDOS

Este país adoptó en 1994 el Acta Federal de Abuso Computacional que modificó al Acta de Fraude y Abuso Computacional de 1986.

En el mes de Julio del año 2000, el Senado y la Cámara de Representantes de este país -tras un año largo de deliberaciones- establece el Acta de Firmas Electrónicas en el Comercio Global y Nacional. La ley sobre la firma digital responde a la necesidad de dar validez a documentos informáticos -mensajes electrónicos y contratos establecidos mediante Internet- entre empresas (para el B2B) y entre empresas y consumidores (para el B2C).

3. TERRORISMO COMPUTACIONAL

   El tema del terrorismo computacional o mejor el ciberterrorismo, dado que este tipo de pánico se genera haciendo uso de la Internet. Un computador es por definición una herramienta magnifica que ha evolucionado y lo sigue haciendo para ayudarnos y facilitar nuestro trabajo. Sin embargo la delincuencia se ha dado mañas de utilizarlos como armas en función del terrorismo, y esto se da cuando se utiliza para generar terror, como extorciones o simplemente para asustar, entre muchas más cosas. Es importante entonces que hagamos un uso adecuado de nuestros equipos y sistemas de cómputo, sea en las empresas o en los hogares, definir políticas claras para un uso adecuado y en las empresas especialmente los procesos y procedimientos para manipular equipos o accesar a la información.

4 Definición

El spyware o programa espía: es un software que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador. El término spyware también se utiliza más ampliamente para referirse a otros productos que no son estrictamente spyware. Estos productos, realizan diferentes funciones, como mostrar anuncios no solicitados (pop-up), recopilar información privada, redirigir solicitudes de páginas e instalar marcadores de teléfono.

Malware: también llamado badware, código maligno, software malicioso o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o Sistema de información sin el consentimiento de su propietario. El término malware es muy utilizado por profesionales de la informática para referirse a una variedad de software hostil, intrusivo o molesto. El término virus informático suele

aplicarse de forma incorrecta para referirse a todos los tipos de malware, incluidos los virus verdaderos.

Hoax: es un correo electrónico distribuido en formato de cadena, cuyo objetivo es hacer creer a los lectores, que algo falso es real. A diferencia de otras amenazas, como el phishing o el scam; los hoax no poseen fines lucrativos, por lo menos

Antivirus : Al ejecutarlos 'siempre' nos van a mostrar alguna falsa infección o falso problema en el sistema que si queremos arreglar vamos tener que comprar su versión de pago… la cual obviamente en realidad no va a reparar ni desinfectar nada, pero nos va a mostrar que sí.

En conclusión

Bien, es importante entonces teniendo en cuenta lo mencionado, ser consientes del manejo adecuado de información, de una protección fuerte en todo sentido, de una declaración clara de políticas y procedimientos y especialmente de una selección exhaustiva del personal informático.

Pero más aún saber que debemos prepararnos constantemente y estar actualizándonos al respecto de la seguridad informática y todo lo que esto implica, porque así como la tecnología y el mundo evoluciona, también lo debemos hacer nosotros dado que el crimen también lo hace.

BIBLIOGRAFIA

es.wikipedia.org/wiki/Malware

http://es.wikipedia.org/wiki/Delito_inform%C3%A1tico

http://sena.blackboard.com/webapps/portal/frameset.jsp?tab_tab_group_id=_7_1&url=%2Fwebapps%2Fblackboard%2Fexecute%2Flauncher%3Ftype%3DCourse%26id%3D_308908_1%26url%3D

http://www.monografias.com/trabajos/legisdelinf/legisdelinf.shtml

http://www.monografias.com/trabajos6/delin/delin2.shtml#audi

http://www.gobiernoelectronico.org/node/5207

http://seguridad.internet2.ulsa.mx/congresos/2003/cudi2/legislacion.pdf

http://seguridad.internet2.ulsa.mx/

ttp://www.gestiopolis.com/recursos/documentos/fulldocs/fin1/papetrabbetty.htm