LA SEGURIDAD DE LA INFORMACIÓN RESPONSABILIDAD DE TODOS

Ingeniero Ricardo A. López Bulla

En este artículo se realiza una reflexión sobre el manejo de la información y la seguridad de la misma y se dan algunas recomendaciones para no ser víctima de los delincuentes.

Abstract

This article is a reflection on the management of information and security of it and give some recommendations to avoid being a victim of criminals.

Palabras Claves

Seguridad, TIC, Phishing, delito informático, Crimeware.

Una primera mirada

En Colombia la seguridad de la información ha estado en un segundo plano no existe la conciencia corporativa, ni se le da la importancia que esta tiene, la pequeña y mediana empresa no invierte en capacitación a usuarios finales que en últimas son los responsables de la información. En un estudio realizado por Kaspersky Lab y por la agencia B2B International , revela que Solo el 46% de las compañías capacitan a sus usuarios finales sobre cómo deben acceder de manera segura los datos en la nube, el 82% de las compañías ha implementado protección de malware. Así mismo, el 80% tienen instaladas medidas contra el spam. Pero solo dos de cada cinco organizaciones usan tecnologías verdaderamente eficientes para protegerse contra las amenazas corporativas, Por tal razón la seguridad debe convertirse en una prioridad de cualquier departamento de TI.

La ley 1273 de 2009 Por medio de la cual se modifica el Código Penal, y crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”, busca preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, y penaliza con prisión entre 36 a 96 meses y multas de 100 a 1000 salario mínimos legales diarios vigentes a quienes incurran en estos delitos.

Asegurando la información personal

Si esto sucede a nivel empresarial ¿qué ocurre a nivel personal?, en este aspecto es aún más preocupante la situación, se suele creer los hacker , cracker , solo atacan las grandes compañías, pero resulta que cualquier persona con algún interés particular puede obtener programas de fácil manejo que le permitan acceder a claves, cuentas de correos del usuario, numero de cuentas bancarias con sus respec-

Información drindada por Kaspersky Lab en comunicado de prensa mayo de 2013 recopidado de http://latam.kaspersky.com/ar/sobre-kaspersky/centro-de-prensa/comunicados-de-prensa/solo-2-de-cada-5-organizaciones-usan-tecnolog

tivas contraseñas y a mucha más información personal.

Estas vulnerabilidades son en su gran mayoría errores de usuario, los cuales tiene malos hábitos de seguridad en el manejo de información, en el simple uso de claves los usuarios cometen errores como el de asignar claves predecibles (nombres de los hijos, fechas de nacimiento, placa del vehículo, etc…) información que mucha gente conoce, o aun peor claves numéricas como 1234, 9876, 1357 etc.

Que en un ataque de criptoanálisis es lo primero a lo que se recurre, o con programas sniffer que nos permiten capturar la información que viaja por la red.

Otra técnica muy común de ataque es la Ingeniería Social la cual está definida como la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos, haciendo uso de la persuasión, muchas veces abusando de la ingenuidad o confianza de un usuario, para obtener información que pueda ser utilizada para tener acceso autorizado a la información de las computadoras y/o a sistemas de información que les permitan realizar algún acto que perjudique o exponga a personas u organismos.
Ejemplo de estos hay muchos uno de los más usados es él envió de mensajes al correo en donde el remitente dice ser el gerente del banco o un miembro de seguridad del mismo y se le pide al usuario que por medio de un LINK que ellos proporcional introduzca todos los datos, incluyendo claves, números de verificación, número de tarjeta, etc… estos mensajes siempre vienen acompañados de coacción por ejemplo "DE HACER CASO OMISO A ESTE MENSAJE EL BANCO NO SE HACE RESPONSABLE DE LA PERDIDA DE SU DINERO" , lo cual atemoriza al usuario y lo incita a realizar de inmediato la acción que se le pide, Sin darse cuenta que a la página que lo lleva ese link no es la página del banco si no una página parecida que han creado los criminales para capturar la información, a esta técnica se le llama Phishing

No bastan las campañas publicitarias que las entidades bancarias realizan en la prevención de delitos informáticos los clientes caen por cantidades.

Otra técnica común en delitos informáticos es el uso de software malicioso denominado Crimeware , entre estos tenemos los capturadores de pulsación como los Keylogger los cuales registran y guardan todo lo que un usuario pulse en el teclado y lo envía a un archivo el cual puede ser transmitido por internet. Otros malwares como troyanos, permiten que el ciber criminal tome el control de la maquina y/o la redireccione a una página replica de un sitio web.

Sin ir más lejos la publicación de información personal en las redes sociales como Facebook, Twitter, etc permiten que personas ajenas obtengan gran cantidad de información personal la cual en cierto momento puede ser utilizada para manipulación de otras personas y es elemento fundamental en la ingeniería social, y si a esto le sumamos que existen bases de datos como las de las EPS, en internet las cuales pueden ser

Hacker especialistas en informática que utilizan sus conocimientos con el fin de detectar cualquier tipo de vulnerabilidad, errores o fallos de seguridad, etc. para poder solucionarlos y evitar posibles ataques. (Hacking – Ético)

Cracker o Black Hat, hace referencia a expertos en seguridad informática que tratan de detectar las debilidades o deficiencias de programas y equipos informáticos, para obtener algún tipo de beneficio.

accedidas por cualquier persona y obtener al instante la información, podemos concluir sin mucho esfuerzo que nuestra información está en peligro.
En Colombia el riesgo es mayor porque no existe la cultura de consultar las cuentas personales desde un solo computador. La gente usa el de la oficina, la universidad, el café internet y no tienen una sesión personalizada en el de la casa, por lo cual sus datos están expuestos a ser 'hackeados' fácilmente, a esto agreguémosle la costumbre de conectarnos a redes WiFi públicas y/o abiertas las cuales nos advierten que NO son seguras, pero de igual forma nos conéctanos pensando " Internet Gratis" y colocamos en mayor riesgo la integridad, confidencialidad y disponibilidad de la información.

La invitación es a tomar las medidas mínimas preventivas en el manejo de la información y no ser un número más de las víctimas de los ciber criminales pasando a engrosar las estadísticas de la policía.

Recomendaciones y consejos de seguridad:

- Instalar software legal y mantener actualizados los parches de seguridad.
- No descargar aplicaciones de tiendas online que no sean oficiales.
- Si se conecta por un Wi-Fi abierto o público, nunca ingresar a una red social o una cuenta de correo, porque uno no sabe por dónde viaja esa información.
- Cuando no se utiliza el Bluetooth o el Wi-Fi, lo mejor es desactivarlo.
- La regla de oro, Nunca entregue sus datos por correo electrónico. Las empresas y bancos jamás le solicitaran sus datos financieros o de sus tarjetas de crédito por correo.
- No ingrese por medio de link a las páginas de los bancos, entidades financieras, redes sociales, siempre digite el dirección en la URL
- Si recibe un email tipo de phishing, jamás lo responda. Denuncie ante las autoridades.
- No descargue ni ejecute archivos de procedencia desconocida.
- Si al instalar un software le informa que no cumple los certificados de seguridad o que no está firmado digitalmente, esto le está indicando que el programa fue alterado NO lo instale.
- No proporcione información confidencial a través de la red.
- Cerciórese de siempre escribir correctamente la dirección del sitio web que desea visitar ya que existen cientos de intentos de engaños de las páginas más populares con solo una o dos letras de diferencia.
- Establezca reglas en el uso de internet
- Instale un buen software antivirus y manténgalo actualizado
- Compruebe que la página web en la que ha entrado es una dirección segura y ha de empezar con https:// y un pequeño candado cerrado debe aparecer en la barra de estado de nuestro navegador.
- Recuerde nadie da nada gratis y menos en la red.

Phishing: Técnica utilizada para captar datos bancarios de los usuarios a través de la utilización de la imagen de la entidad bancaria.
Crimeware herramientas de software utilizadas en los crímenes cibernéticos.