MEDICIEGO 2007; 13(Supl.2)
ISSN: 1029-3035 RNPS: 1821

La informática ha llegado a nuestras vidas
Computer science has come into our lives

Ciego de Ávila, julio 2007.
"Año 49 de la Revolución"

De: Ing. Rigoberto Borroto Pacheco.
Dpto. Computación.
Facultad de Ciencias Médicas de Ciego de Ávila

A: Dra. Yolanda Pérez Jiménez
Directora Revista Provincial MediCiego

Dra:

La Informática ha llegado a nuestras vidas y las nuevas tecnologías de la informática y las telecomunicaciones (TIC) han venido a nosotros, además, como herramientas de trabajo para facilitarnos lo que hace años era muy difícil de lograr, pero en la misma medida en que las nuevas tecnologías favorecen y enriquecen nuestro trabajo diario, crean nuevas preocupaciones.

Quiero compartir con usted una preocupación relacionada con el inadecuado uso de las TIC. El robo, falsificación y modificación de información es tarea cotidiana y delito perseguido en el mundo. En mayor o menor escala, somos víctimas también del uso de aplicaciones no autorizadas y podemos ser blanco directo de la mala intención de una o varias personas. Nuestro medio no queda exento de tales ataques, el intento de robo de un examen no deja de ser una meta para algunas personas. También es el caso de otros documentos tan importantes como ese.

Específicamente reflexiono sobre el robo de información procesada en una PC. Individuos mal intencionados aprovechan la negligencia o el desconocimiento para apropiarse y dar uso a información de terceros.

Hace unos años cuando una simple PC era un equipo aislado y donde sus puertos de entrada y salida solían ser simples disquetes las preocupaciones eran grandes en las personas que estaban a cargo de esta información, pensando en el robo, modificación falsificación o uso mal intencionado de la misma. Hoy, cuando la información viaja a grandes o bajas velocidades por las redes y cuando existen medios externos que pueden ser mayores a la capacidad de almacenamiento de una PC, las preocupaciones crecen. Una memoria externa USB es cada día más natural hallarla entre nuestros compañeros de trabajo, amigos y conocidos. La información viaja de PC en PC, enviada por email, bajada de sitios FTP, copiada o transportada desde un centro a otro en una memoria flash, en un disco externo, en un DVD, CD u otro medio.

Pienso que cada medida que tomemos es importante, incluso si se tomasen medidas extremas. El principal riesgo que identifico es el procesamiento en un área no autorizada, el no tener una computadora en la oficina nos obliga a usar una que nos ceden por una hora o dos para realizar dicha actividad, incluso imprimimos en ese lugar.

El riesgo es muy alto si estamos conectados a la intranet o la red de redes. Pudiéramos recibir ataques accidentales o maliciosos. No voy a hablar de virus informáticos que bien podrían hacernos pasar un mal rato e incluso provocar una situación desesperada, voy a referirme a un ataque malicioso, planificado e inteligente, que pudiera ir dirigido a personas que apenas conocen los sistemas, pero

pudieran estar dirigidos también a personas altas conocedoras de estos temas y perfectamente ser timadas directa o indirectamente.

Es bien difícil para cualquier persona hoy asegurar que sus datos no van a ser leídos por personas no autorizadas. Para evitar el robo de información vital grandes compañías destinan milllonarias sumas, e incluso así han sido vendidos sus datos de forma no autorizada, veamos el caso Cisco Systems de abril de 2001, cuando dos de sus empleados fueron acusados de obtener acceso no autorizado a títulos de Cisco y obtuvieron 6.3 millones de dólares de forma ilegal (1).

Es sencillo apropiarse en nuestro medio de tales datos, somos irresponsables y propiciamos el robo pues la información no está encriptada ni posee contraseñas, usualmente la manipulamos y la llevamos en el bolsillo, la cartera, o suspendida del cuello, la computadora donde nos sentamos pertenece a un lugar totalmente monitoreado por técnicos, administradores de red y otro personal debidamente autorizado y en quienes debemos confiar.

Lo que más comúnmente encontramos es que el propietario, personalmente, elimina la información del disco duro y verifica además que dicha información haya sido “definitivamente eliminada” de la llamada papelera de reciclaje de los sistemas operativos de Microsoft. Hacer esto carece de valor alguno, diversos softwares son capaces de rescatar esta información, incluso después de haber formateado la unidad (2).

El acceso a sus datos en el momento de que usted está procesando la información constituye en nuestro medio el miedo más difundido y contra él hemos tomado tantas medidas que no valen la pena mencionar, todas son correctas, pero ¿de qué vale tener a una persona confiable allí con nosotros si una vez terminado el proceso conectamos nuevamente a la red? Si estuvo en disco duro la información que ya no procesamos de seguro podremos acceder a la misma. Sería bastante sencillo robar la contraseña del dueño de la PC con un simple software. El resto sería labor de principiantes, los softwares están diseñados para usuarios finales que perdieron su información por error, por tanto, son tan sencillos de utilizar que con tenerlo instalado bastaría para obtener los resultados esperados.

Es difícil brindarle una guía definitiva que cuando usted la aplique quede seguro de que sus datos no serán robados, si el sistema funciona bien y no le hablo del sistema operativo, nuestras preocupaciones serían mínimas.

Un usuario experto ante esta situación haría lo siguiente: desconectaría el cable de red, teclearía él mismo el documento en una oficina con las condiciones necesarias y solamente salvaría dicha información en medio externo que trasportaría todo el tiempo con él. El documento que porta le pondría contraseña que debería cumplir requisitos especiales en cuanto a su complejidad. En dependencia del destino de esta información podría encriptarse o no, esto ya dependería de su futuro uso. Se imprimiría un ejemplar que con todas las medidas se transportaría a reproducir y allí tomaría todas esas medidas que finalizan en la recogida del master y que, si aplicamos bien, después vendrían otras medidas que tampoco son informáticas y por tanto no las referiré, pero le comento, y solo para preocuparla le digo, alguien pudo robar sus datos.

Existen software espías que pudieron ser instalados en su sistema y que lo está espiando a usted todo el tiempo, monitoreando cada vez que usted toca una tecla, inserta una palabra clave y además fotografía constantemente su escritorio o ventana principal activa, este software “indetectable” puede ser revisado después y pudiera obtenerse de forma parcial o total la información que usted tanto ha cuidado (3).

Otras vías existen para robar sus datos, pero no pretendo que esto sea una revisión bibliográfica, pretendo llamar la atención y alertar sobre el peligro que enfrentamos cuando usamos las nuevas tecnologías y confiamos en la honestidad de todos. Desconfiar inicialmente de nuestra capacidad para evitar el robo de la información que procesamos es vital, para ello tomemos las medidas necesarias.

La administración debe confiar en las personas que se han ganado el mérito para estar al frente de tamañas tareas, la honestidad debe primar en la persona que nos ayuda con la reproducción, manipulación, digitalización del documento, pero nos corresponde a nosotros, dueños y máximos responsables de nuestros datos, exigir y velar por la integridad de nuestra información. Será preciso que seamos nosotros mismos quienes tecleemos, protejamos al extremo y manipulemos nuestra información, evitando tener que confiar otras personas. Los datos jamás serán guardados en discos duros y cuando por alguna razón sea necesario se tomarán medidas usando contraseña, encriptación y le sugerimos además confundir al atacante usando un nombre de fichero y carpeta no sospechosa, pudiera ser modificada la extensión de dicho fichero y con ello falseamos aún más la información a primera vista.

Evitaremos a toda costa que este fichero será enviado a través del email y se informará al responsable de seguridad informática cuando pensemos que alguna irregularidad puede o podría suceder.

Si me pide una fórmula, le puedo dar una, aunque no la considero totalmente perfecta. Le recomiendo tener una PC aislada con una persona totalmente responsable sin contraseñas de administración y un software espía instalado que será revisado por un personal especializado cada cierto tiempo por una comisión o como quiera implementarse, allí se realizaría el total procesamiento e impresión. El software de monitoreo, y ¿por qué no hacerlo? comento a todos que está instalado.

Referencias bibliográficas

1- Confianza en el ciberespacio: Cómo construir un mundo en línea lícito y seguro. [sitio en Internet] 2007 [citado 1 May 2007] [aprox. 2 pantallas]. Disponible en: http://w3.bsa.org/seguridad/issue/.

2- Propiedad intelectual, Seguridad Informática. [sitio en Internet]2007 [citado 12 May 2007] [aprox. 1 pantallas]. Disponible en: http://w3.bsa.org/seguridad/issue/

3- Hacker! = Cracker. [sitio en Internet] 2007 [citado 7 Jun 2007] [aprox. 1 pantallas]. Disponible en: http://www.microsiervos.com/archivo/internet/hacker-cracker.html