Boletín 1-2001, artículo 2º

Seguridad Informática

Gustavo Rojas García
Sección de Auditoría Informática

La gran competitividad entre las empresas que fabrican equipos de cómputo (hardware) ha favorecido la oferta en el mercado de productos con mayores capacidades y contribuido a la baja de precios.Esta misma situación se presenta en el sector de la comercialización de programas de cómputo (software).Como consecuencia de esta dinámica, el grado de dependencia que en general tienen las organizaciones de la tecnología informática se ha incrementado notoriamente.Aunado a esta dependencia, también se presenta el fenómeno de la rapidez y continuidad en los avances que ha caracterizado esta rama de la ciencia.

Sin lugar a dudas, de estas circunstancias se han beneficiado los propios consumidores, los que adquieren mejores equipos y programas para apoyar no solo sus labores cotidianas, sino que también pueden efectuar otras que antes no era posible realizar, por ejemplo: la flexibilidad para el intercambio de archivos a nivel mundial, por medio de la InterNet.No obstante lo señalado anteriormente, se debe prestar especial atención a este tipo de adquisiciones, ya que además de los beneficios que se esperan obtener,también pueden eventualmente generarse situaciones no deseadas, entre ellas las relacionadas con los problemas de seguridad informática.Dependiendo de su magnitud, un problema de seguridad informática, puede llegar a comprometer la continuidad de las operaciones de una oficina, de un departamento o en el peor de los casos de toda una Organización.

Debido a las características propias de la nueva tecnología, los problemas de seguridad informática no solo atañen a la parte técnica, sino que también llegan al ámbito de los usuarios de los sistemas de información.

A continuación enumeramos, tres aspectos o puntos débiles que podrían comprometer la integridad de la información almacenada en los principales equipos de cómputo de la Universidad:

1. Mal uso de las palabras claves de acceso

Las palabras claves o password, que muchos usuarios están acostumbrados a digitar, se utilizan para identificar y restringir el acceso a los sistemas deinformación.

En muchos casos, los usuarios, por desconocimiento o descuido, escogenpalabras de acceso muy fáciles de descifrar, por ejemplo: su número de cédula, las iniciales de su nombre, o bien las tienen escritas en lugares visibles por lo que pueden ser leídas por otras personas.Además, muchos usuarios facilitan sus claves de acceso a otros compañeros de trabajo para que también utilicen los sistemas.

Una buena recomendación es motivar a los usuarios para que escojan claves fáciles de recordar solamente para ellos mismos, pero bastante difíciles de conseguir para otras personas.Además, las claves deben tener una longitud mínima de 8 caracteres y deben ser una combinación de letras y números.Por ejemplo:grg63260.

Además, el personal técnico informático debe capacitar constantemente a los usuarios para que escojan palabras clave adecuadas y hacer conciencia en ellos de que estas claves de acceso son confidenciales (deben ser utilizadas únicamente por su dueño) por lo que no deben divulgarse a terceras personas por motivo alguno.

2. Contagio por virus

La popularidad del correo electrónico representa un punto de mucho cuidado para el personal informático,ya que por medio del e-mail pueden ingresar los denominados virus informáticos, que son programas de los que todos los días oímos hablar.Entre los daños que pueden ocasionar los virus, está la pérdida de información almacenada en nuestros computadores.

Un buen ejemplo de estos peligrosos programas es el denominado virus I Love You, que viene dentro de un e-mail con el subject ILOVEYOU.Este virus se encuentra dentro del archivo LOVE-LETTER-FOR-YOU.TXT.VBS, el cual se retransmite automáticamente a todas las direcciones de la lista de correos del usuario y su objetivo es destruir todos sus archivos.Otro archivo que lo contiene se llama WIN-BUGSFIX.exe.Se sabe que este virus ha cambiado de nombre, ahora sus alias son: joke, very funny, spider, entre otros.

Para evitar el contagio por virus es recomendable que el personal informático mantenga un constante flujo de avisos a los usuarios, informándoles acerca de la aparición de nuevos virus.También es importante que los usuarios conozcan las herramientas informáticas para la limpieza de los virus y que las puedan utilizar paradesinfectar sus máquinas y así evitar su propagación a otros computadores.

3. Ingreso de intrusos

Los intrusos son personas que pueden ser funcionarios de la propia universidad o ajenos a ella, que no cuentan con la debida autorización para acceder información propiedad de la Universidad.Para lograr el acceso a esta información, hacen uso de claves de acceso prestadas, ilegalmente adquiridas o bien se aprovechan de fallas aún no detectadas en la seguridad de los sistemas.

Los motivos que alientan a un intruso son muy variados y van desde la simple curiosidad, hasta actos malintencionados como lo son el borrado de datos,la sustitución de valores en registros determinados y el copiado de información confidencial para divulgarla posteriormente.Se sabe que un intruso puede actuar por diversas razones; una de ellas podría ser vengarse de la propia organización, por lo cual en situaciones especiales (despidos,

suspensiones, traslados, entre otros), la Jefatura debe comunicar oportunamente al personal informático para que proceda a desactivar los privilegios de acceso a los sistemas.

Como funcionarios universitarios, debemos hacer conciencia para mantener niveles aceptables de seguridad y proteger adecuadamente la información.No sólo dependemos de la tecnología (software y hardware) sino que también del grado de colaboración que podamos aportar a los técnicos y profesionales en informática, con el propósito de que ellos evalúen los problemas encontrados y tomen las acciones y prevenciones del caso.

La información almacenada en losEquipos de Cómputo de la Universidad de Costa Rica constituye un activo sumamente valioso que permite la continua prestación de los múltiples y variados servicios que brinda nuestra Institución a la comunidad universitaria, por lo que todos debemos velar por el mantenimiento de un adecuado ambiente de seguridad informática para su protección.

Igualmente, el resto de los elementos que intervienen en la captación, procesamiento, entrega, uso y distribución de la información, deben protegerse contra la destrucción, modificación, utilización y divulgación no autorizada.

Esperamos que este artículo constituya un punto de partida para la reflexión y el debate sobre los problemas en seguridad informática que eventualmente puedan presentarse en nuestra Institución y de la implementación de las soluciones.