AMENAZAS INFORMÁTICAS Y SEGURIDAD DE LA INFORMACIÓN

*César H. Tarazona T.**

ASPECTOS GENERALES

Casi todas las organizaciones públicas o privadas, al igual que las personas, dependen de alguna manera de la tecnología de la información como una herramienta esencial para lograr sus objetivos de negocio o para poder desarrollar actividades en su vida cotidiana; al mismo tiempo, todos tienen que enfrentarse con una amplia gama de amenazas y vulnerabilidades asociadas a los entornos informáticos de hoy.

La seguridad de la información es más que un problema de seguridad de datos en los computadores; debe estar básicamente orientada a proteger la propiedad intelectual y la información importante de las organizaciones y de las personas.

Los riesgos de la información están presentes cuando confluyen dos elementos: amenazas y vulnerabilidades. Las amenazas y vulnerabilidades están íntimamente ligadas, y no puede haber ninguna consecuencia sin la presencia conjunta de éstas. Las amenazas deben tomar ventaja de las vulnerabilidades y pueden venir de cualquier parte, interna o externa, relacionada con el entorno de las organizaciones.

Las vulnerabilidades son una debilidad en la tecnología o en los procesos relacionados con la información, y como tal, se consideran características propias de los sistemas de información o de la infraestructura que la contiene. Una amenaza, en términos simples,

* Consultor en Seguridad de la Información, Etek Internacional.

es cualquier situación o evento que puede afectar la posibilidad de que las organizaciones o las personas puedan desarrollar sus actividades afectando directamente la información o los sistemas que la procesan.

TIPOS DE AMENAZAS

Básicamente, podemos agrupar las amenazas a la información en cuatro grandes categorías: Factores Humanos (accidentales, errores); Fallas en los sistemas de procesamiento de información; Desastres naturales y; Actos maliciosos o malintencionados; algunas de estas amenazas son:

- Virus informáticos o código malicioso
- Uso no autorizado de Sistemas Informáticos
- Robo de Información
- Fraudes basados en el uso de computadores
- Suplantación de identidad
- Denegación de Servicios (DoS)
- Ataques de Fuerza Bruta
- Alteración de la Información
- Divulgación de Información
- Desastres Naturales
- Sabotaje, vandalismo
- Espionaje

A continuación se presenta la descripción de algunas de de las principales amenazas:

• *Spywre* (Programas espías): Código malicioso cuyo principal objetivo es recoger información sobre las actividades de un usuario en un computador (tendencias de navegación), para permitir el despliegue sin autorización en ventanas emergentes de propaganda de mercadeo, o para robar información personal (p.ej. números de tarjetas de crédito). Hay iniciativas de utilizarlos para controlar el uso de software pirata.
Según algunas estadísticas, cerca del 91% de los computadores tienen spyware instalado, y de acuerdo a un reporte de la firma EarthLink", en una revisión de cerca de 1 millón de computadores en Internet, el promedio de programas "spyware" en cada uno era de 28.
• *Troyanos, virus y gusanos*: Son programas de código malicioso, que de diferentes maneras se alojan el los computadores con el propósito de permitir el acceso no autorizado a un atacante, o permitir el control de forma remota de los sistemas. El virus, adicionalmente, tiene como objetivo principal ser destructivo, dañando la información de la máquina, o generando el consumo de recursos de manera incontrolada para bloquear o negar servicios.

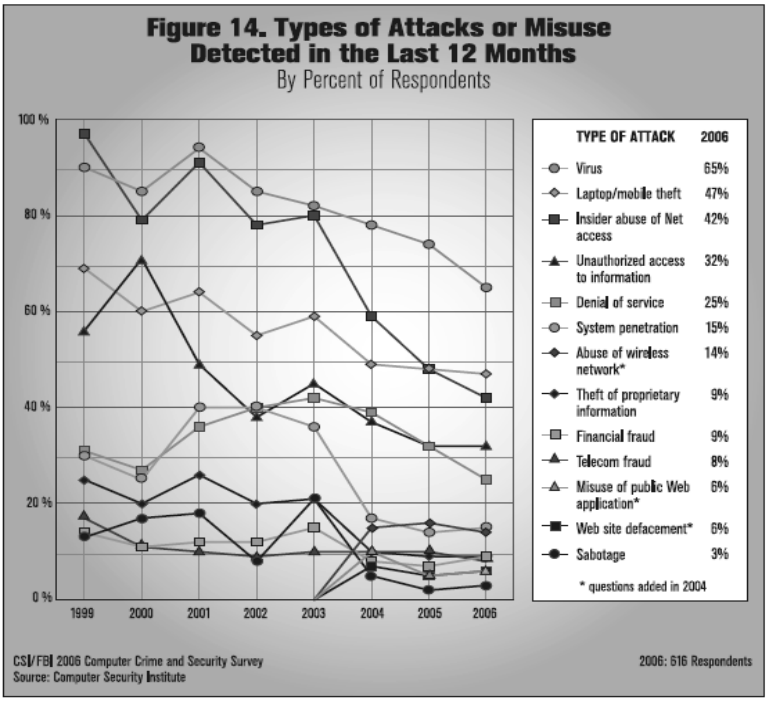
El vector de propagación de estos códigos es, casi siempre, otro programa o archivo (un programa ejecutable, imagen, video, música, reproducciones flash, etc.); de otra parte, los virus, se replican ellos mismos una vez instalados en el sistema.
Las estadísticas indican que mensualmente se generan cientos de estos programas, cuyo principal objetivo es robo financiero, poniendo en riesgo la información confidencial y el dinero de las personas y de las organizaciones, más que la destrucción de archivos.
La última tendencia en clases de virus se denomina cripto-virus, el cual, una vez instalado, cifra la información contenida en el disco del equipo, o algunos archivos contenidos en éste, y posteriormente se solicita una cantidad de dinero para que sus autores entreguen las claves para recuperar el contenido de los archivos cifrados (secuestro express de la información).
• *Phishing*: Es un ataque del tipo ingeniería social, cuyo objetivo principal es obtener de manera fraudulenta datos confidenciales de un usuario, especialmente financieros, aprovechando la confianza que éste tiene en los servicios tecnológicos, el desconocimiento de la forma en que operan y la oferta de servicios en algunos casos con pobres medidas de seguridad.
Actualmente, los ataques de phishing son bastante sofisticados, utilizando mensajes de correo electrónico y falsos sitios Web, que suplantan perfectamente a los sitios originales.
• *Spam*: Recibo de mensajes no solicitados, principalmente por correo electrónico, cuyo propósito es difundir grandes cantidades de mensajes comerciales o propagandísticos. Se han presentado casos en los que los envíos se hacen a sistemas de telefonía celular – mensajes de texto, o a sistemas de faxes.
Para el año 2006, se tenía calculado que entre el 60 y el 70% de los correos electrónicos eran "spam", con contenidos comerciales o de material pornográfico.
Según la compañía Symantec, el tipo de spam más común en el año 2006 fue el relacionado con servicios financieros, con cerca del 30% de todo el spam detectado.
• *Botnets* (Redes de robots): Son máquinas infectadas y controladas remotamente, que se comportan como "zombis", quedando incorporadas a redes distribuidas de computadores llamados robot, los cuales envían de forma masiva mensajes de correo "spam" o código malicioso, con el objetivo de atacar otros sistemas; se han detectado redes de más de 200.000 nodos enlazados y más de 10.000 formas diferentes de patrones de "bots".
Las organizaciones deberían revisar los computadores de sus redes de datos para detectar síntomas de infecciones relacionadas con este patrón, para evitar ser la fuente de ataques hacia otras redes o sistemas. También se requiere de la colaboración y aporte permanente de los usuarios finales y de los proveedores de acceso a Internet y prestadores de servicios como los "café Internet".
• *Trashing:* Un método cuyo nombre hace referencia al manejo de la basura. No es una técnica relacionada directamente con los sistemas de información, pues los atacantes se valen de otra forma de ingeniería social y para ello, el mecanismo utilizado, es la búsqueda en las canecas de la basura o en los sitios donde se desechan papeles y documentos de extractos bancarios, facturas, recibos, borradores de documentos, etc., y posteriormente utilizarla según convenga, elaborando un perfil de la víctima para

robar su identidad, o teniendo acceso directamente a la información que se suponía confidencial.

ATAQUES INFORMÁTICOS

Según los datos de la encuesta anual de Seguridad del FBI[1], los virus informáticos siguen siendo la principal fuente de pérdida financiera en las organizaciones, seguidos por los impactos derivados de accesos no autorizados a los sistemas, el robo de información de propiedad industrial, y la pérdida de computadores personales o elementos de computación móvil. Estas causas generan más del 74% del total de las pérdidas financieras.

Las inversiones en tecnología para protección en seguridad informática cada día aumentan, y aún así, se presentan resultados como los mostrados en la encuesta e ilustrados en la siguiente gráfica; las situaciones de inseguridad informática o de la información no se dan solo por personas descuidadas que divulgan información confidencial, se dan en grandes empresas multinacionales, que cuentan con departamentos de tecnología y recursos suficientes para invertir en protección. Entonces, ¿cuál es la falla?



1 CSI/FBI Computer Crime and Security Survey - 2006

Según un reciente estudio publicado por AvanteGarde[2], que realizó una prueba consistente en dejar unos sistemas conectados a Internet con las protecciones básicas configuradas de fábrica, el tiempo promedio en el que un equipo resultó "exitosamente" atacado fue de solo 4 minutos.

La primera cosa que una persona hace con un computador nuevo es conectarlo a Internet, enviar correos, bajar archivos (música, videos, etc.), navegar, jugar, "chatear", y otras cosas; nadie piensa en la seguridad del equipo, instalar parches y herramientas de protección. (Firewall personal, antivirus, anti-spam, copias de respaldo).

La falla principal que permite que los usuarios sean atacados y sean víctimas de la gran cantidad de amenazas que nos acechan, radica en que en muchos casos no se está gestionando la tecnología dentro de un marco completo de protección de la información, y en la falta de concientización a las personas en los riesgos relacionados con el uso de tecnología y de herramientas como Internet, por lo que los esfuerzos se pierden o se orientan a cumplir objetivos imprecisos. Las inversiones en tecnología de seguridad, como solución a los problemas planteados, deben ser realizadas dentro de un marco sincronizado con otra serie de medidas para formar lo que se conoce como un "Sistema de Gestión de Seguridad de la Información".

IDENTIFICACIÓN EN LA RED

Todos los sistemas informáticos conectados en red poseen identificadores para poder enviar y recibir la información desde otros sistemas. Esta identificación se conoce como la dirección IP (Internet Protocol).

Para que un sistema pueda acceder a Internet, necesita tener una dirección IP única, que no se repita o que no posea otro sistema en la red. Para situaciones normales como envío de correo ofensivo, navegación, descarga de archivos, conversación con otros usuarios, es posible encontrar el rastro dejado por el computador utilizado, y en algunos casos logar detectar su ubicación física.

La red no es totalmente anónima, pero para lograr la identificación se requiere en muchos casos de la colaboración de diferentes entidades como los proveedores de acceso a Internet y las empresas que prestan servicios de alojamiento de páginas Web.

Los sistemas informáticos utilizan niveles pobres de autenticación tanto de sistemas como de usuarios, lo cual disminuye la posibilidad de actuar contra los atacantes. Para ataques elaborados como envío de spam, virus o inclusive accesos no autorizados, los atacantes han desarrollado técnicas que permiten utilizar direcciones simuladas o

---

2 Security Absurdity: The complete, unquiestionable, and total failure of information security.

falsas, cambiando la dirección original asignada, y de esa forma engañar los procesos de búsqueda e identificación y en mucos casos se valen de servidores públicos, para que en caso de ser identificados, se puedan mover fácilmente a otros sistemas sin dejar rastro, y continuar con sus ataques.

LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

"La información es un activo que, al igual que otros activos del negocio, es esencial para la organización, y por lo tanto debe ser protegido de forma adecuada." [3]

La *OCDE*[4] desarrolló por primera vez en 1992 una serie de Directrices para la Seguridad de los Sistemas de Información, las cuales tratan de promover el uso y desarrollo de una cultura de la Seguridad, no solo en el desarrollo de Sistemas y Redes de comunicación, sino mediante la adopción de "nuevas formas de pensamiento y comportamiento en el uso de la interconexión de esos sistemas".

Las Directrices presentadas son: Concientización, Responsabilidad, Respuesta Adecuada, Ética, Democracia, Evaluación del Riesgo, Diseño y Realización de la Seguridad, Gestión de Seguridad, Reevaluación.

Con la evolución de los sistemas de información y de la forma de hacer negocios, la información se ha convertido en uno de los activos de mayor valor para las personas y especialmente para las organizaciones. "Los sistemas, redes y servicios de información afines, deben ser fiables y seguros, dado que los participantes son cada más dependientes de estos. Sólo un enfoque que tenga en cuenta los intereses de todos los participantes y la naturaleza de los sistemas, redes y servicios afines, puede proporcionar una seguridad efectiva."

Los objetivos que se buscan con la Gestión de la Seguridad de la Información son la protección de la confidencialidad, integridad y disponibilidad de la información y de los bienes que la contienen o procesan. De esta manera, las organizaciones y personas se pueden proteger de:

---

3 *ISO/IEC 17799:2005*

4 Organización para la Cooperación y el Desarrollo Económico

• Divulgación indebida de información sensible o confidencial, de forma accidental o bien, sin autorización.
• Modificación sin autorización o bien, de forma accidental, de información crítica, sin conocimiento de los propietarios.
• Pérdida de información importante sin posibilidad de recuperarla.
• No tener acceso o disponibilidad de la información cuando sea necesaria

La información debe ser manejada y protegida adecuadamente de los riesgos o amenazas que enfrente. La información valiosa se puede encontrar en diferentes formas: impresa, almacenada electrónicamente, transmitida por diferentes medios de comunicación o de transporte, divulgada por medios audiovisuales, en el conocimiento de las personas, etc.

ISO17799 E ISO27001

Los estándares *ISO 17799 e ISO 27001* le dan a una organización las bases para desarrollar un marco de gestión de la seguridad de la información efectivo, que le permita proteger sus activos de información importantes, minimizando sus riesgos y optimizando las inversiones y esfuerzos necesarios para su protección.

Una de las formas de protección consiste en la aplicación de controles, que en la práctica pueden ser políticas, procesos, procedimientos, organización (definición de una estructura organizacional de seguridad), elementos de software y hardware, mecanismos de protección de la infraestructura física y de seguridad, así como la adecuada selección y entrenamiento del personal que opera y utiliza los recursos de información o informáticos.

La norma ISO 17799 presenta una serie de áreas para ser gestionadas, mediante la aplicación de controles o mecanismos de protección, las cuales van desde la seguridad en los sistemas, pasando por los aspectos de seguridad física, recursos humanos y aspectos generales de la organización interna en las organizaciones.

CUMPLIMIENTO LEGAL

La norma ISO 17799 contiene un capítulo con referencias de buenas prácticas para desarrollar los controles necesarios que se deben aplicar en las organizaciones para tener en cuenta los aspectos legales y regulatorios como parte de la gestión de la seguridad de la información. Un punto importante que se debe tener en cuenta, es la protección adecuada para el uso correcto de los sistemas o recursos informáticos o para evitar el uso indebido de esos recursos, de manera que puedan afectar a terceros (Debida Diligencia).

Aspectos como el cumplimiento y protección de Propiedad intelectual, Derechos de autor, Licencias de software, registros de la organización, información confidencial de clientes, empleados o proveedores, así como el cumplimiento de regulaciones provenientes de organizaciones o entes de control como la Superintendencia Financiera (SARO), Ministerios, Basilea, organismos reguladores de comercio electrónico, ley de "*Habeas Data*", *sox*[5], etc., son aspectos que deben ser incorporados en la definición y aplicación de mecanismos de protección de la información.

Las redes de datos no tienen fronteras físicas y en ocasiones tampoco fronteras legales, por lo que se debe tener especial consideración cuando el flujo de información involucra instituciones situadas en países con regulaciones o normas diferentes, pues lo que en un sitio es ser normal, puede ser indebido o ilegal en otro. Un caso específico es el uso de mecanismos de cifrado, que en algunos países no tiene regulación ni control y en otros es estrictamente prohibido o fuertemente regulado.

CONCIENTIZACIÓN

"… desafortunadamente, las comunidades *underground* son mucho mejores compartiendo información que los profesionales en computación".[6]

Concientización es el nivel de entendimiento que se tiene entre la comunidad de usuarios de un sistema o de la información en sí misma, de los procesos de seguridad para protegerla o de cómo usarla.

El proceso de concientización debe estar orientado a sensibilizar a todas las personas para que identifiquen las amenazas que enfrenta la información y que sigan una serie de reglas o normas para que estas no se materialicen; ellas son quienes crean, utilizan y custodian la información.

---

5 SOX: Sarbanes-Oaxley Act., 2002. – Ley Federal de los Estados Unidos. Acta de reforma de la contabilidad pública de empresas y de protección al inversionista.

6 IRA WINKLER, Presidente de Internet Security Advisors Group.

Es tema de concientización es quizá el punto más neurálgico para obtener buenos resultados en cualquier plan de seguridad de la información, debido a que la persona es casi siempre el punto más débil, por la naturaleza misma del ser humano.

Una de las principales vulnerabilidades actuales se relaciona con la ingeniería social, que es el proceso de convencer a las personas para que divulguen información confidencial. Generalmente se basa en engaños o suplantación de identidad, así como en aparentar tener una autoridad que no es real, de manera que la víctima quede en una situación desprotegida, de la cual no es consciente, y se convierte en ayuda para el atacante; es un proceso muy efectivo, que solo puede ser reducido con entrenamiento y concientización adecuados.

CONCLUSIONES

La información ha sido uno de los elementos claves en el desarrollo y éxito de los negocios y en el desarrollo de la gran mayoría de actividades diarias para los seres humanos. Por esta razón, las organizaciones son cada vez más conscientes de la necesidad de proteger la información de las diferentes amenazas a las que están expuestas.

Hay muchos tipos de amenazas contra los sistemas de información y contra la información en general. No todas las amenazas están relacionadas con delitos informáticos, pero todas, de alguna forma, significan un riesgo para las organizaciones y sus consecuencias deben ser evaluadas. Fallas de Hardware o software, situaciones ambientales o naturales, accidentes, amenazas deliberadas con carácter delictivo como robo o destrucción de propiedad, y en general cualquier tipo de amenazas con origen interno o externo.

La seguridad de la información está orienta a proteger una serie de atributos que principalmente están relacionados con la confidencialidad, integridad y disponibilidad de ésta y por lo tanto a evitar que las amenazas a estas categorías puedan afectar a las organizaciones.

Sin embargo, no hay ninguna medida que pueda garantizar un ambiente libre de amenazas o sin riesgos para la información y para las organizaciones o individuos que la requieren. Por esta razón es que se hace necesario adoptar modelos adecuados de gestión de la seguridad de la información que permitan logar niveles efectivos de protección, basados en la relación coordinada de los diferentes mecanismos existentes, especialmente, los elementos físicos de protección basados en hardware y software, los elementos administrativos como políticas y procedimientos, y el recurso humano que administra, opera y utiliza los recursos informáticos.

Un modelo de gestión ampliamente aceptado es el que se presenta en la norma ISO/IEC 27001:2005, que permite tener un sistema de gestión de la seguridad de la información alineado con los objetivos que las organizaciones tengan para la protección de su

información, con la incorporación de las obligaciones en el cumplimiento de normas, leyes y regulaciones.

Finalmente, el soporte fundamental para lograr los niveles de protección adecuados es una permanente concientización a las personas, para sensibilizarlas en el uso adecuado de los recursos informáticos, en los riesgos propios de su utilización y en la necesidad de adoptar mecanismos de protección que permitan preservar las características básicas de la información de las consecuencias derivadas de posible materialización de los diferentes tipos de amenazas identificadas.

REFERENCIAS BIBLIOGRÁFICAS

SYMANTEC INTERNET SECURITY THREAT REPORT. Trends for July-December 2006.

SECURITY ABSURDITY: The complete, unquestionable and total failure of information security. Noam Eppel, Vivica Information Security Inc.

ISO 27001:2005. Requerimientos para los Sistemas de Gestión de la Seguridad de la Información.

ISO/IEC 17799:2005. Código de práctica para la gestión de la seguridad de la información.

CSI/FBI Computer Crime and Security Survey, 2006.

Los 10 riesgos más comunes para su identidad en línea. RSA Security Inc. http://www.rsa.com/go/idtheft/spanish/fraud.html