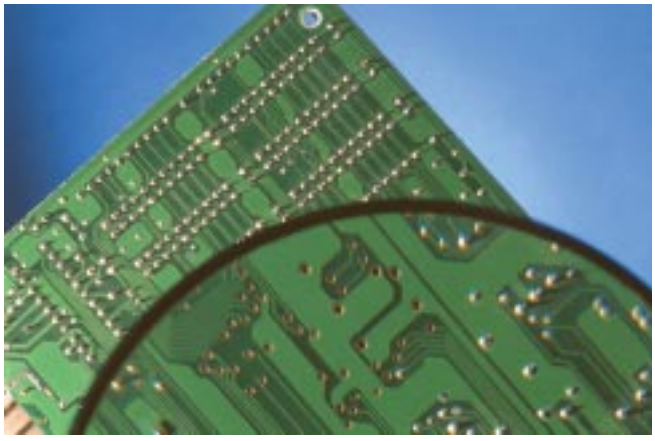
Para tener a la mano

Glosario de seguridad informática



En columnas anteriores hemos visto que los tres pilares básicos de la seguridad de la información son el resguardo de la integridad, confidencialidad y disponibilidad. Ahora presentamos el conocimiento como arma fundamental.

por
Gustavo García Enrich

Sobre la disponibilidad, trató nuestra última columna y el riesgo del fuego como una amenaza latente de suma importancia por su poder destructivo. Como referencia a las dos primeras columnas hemos preparado un glosario de términos afines de uso común en seguridad TI, a manera de introducir a los no especialistas, en la jerga que cada vez se torna más popular dentro de las áreas de sistemas.

La mayoría de los términos se refieren a lo que podríamos denominar Seguridad Lógica, siendo ésta la faceta que más tiempo demanda a los expertos en seguridad. Se han obviado aquellas definiciones puramente técnicas mientras que otras se han simplificado de forma que genere la idea del concepto.

Glosario

A

Activo: Se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga un valor para la organización. Hoy la información es uno de los activos más valiosos de las compañías.

Accidental: Elemento contingente no provocado, casual.

Alerta: Notificación de que se ha producido un incidente relacionado con la seguridad de la información que, de no actuar, en consecuencia puede convertirse en una contingencia mayor.

Análisis de riesgos: Evaluación sistemática de una situación dada para, en base a la información obtenida, identificar las distintas fuentes de riesgo y estimar su probabilidad de ocurrencia. Es posible cuantificar en forma aproximada el valor económico de los riesgos detectados.

Auditoria: Conjunto de procedimientos y técnicas para evaluar y controlar, total o parcialmente, un sistema informático, con el fin de proteger sus activos y recursos.

Ataque de diccionario: Mecanismo utilizado para tratar de descubrir el password (contraseña) de un sistema en el que se prueban todas la palabras recogidas de diccionarios creados a tales efectos y basados en diccionarios idiomáticos.

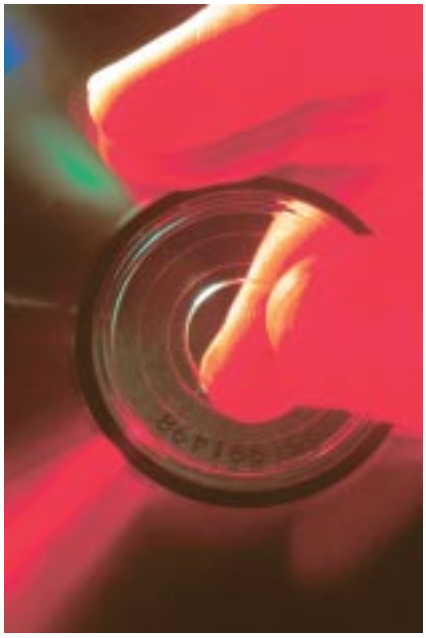
Ataque de fuerza bruta: Mecanismo utilizado para tratar de descubrir el password (contraseña) de un sistema en el que se prueban todas la palabras y combinaciones de letras y números posibles. Ningún sistema puede resistir un ataque de fuerza bruta si se cuenta con el tiempo suficiente. Claves débiles pueden descubrirse en horas pero claves fuertes (alfa numéricas) y largas pueden demandar años (con la capacidad actual de procesamiento pueden ser cientos).

Autenticación: Acción mediante la cual se logra la identificación fehaciente de un individuo o un sistema.

B

BASILEA II: Un nuevo Acuerdo de Capital puesto en marcha a finales del 2006. Según la comunidad de supervisores y de la ban-

ca privada, será una banca más sólida y sensible al riesgo de lo que fue bajo el Acuerdo de Basilea I. En el campo informático calcula el riesgo operativo del negocio por motivo del mal funcionamiento o indisponibilidad de las TI. El Comité de Basilea es también conocido como el "Banco Central de los Bancos Centrales" porque está integrado por representantes de los Bancos Centrales de más de 100 países miembros.



BS7799: Conocido como *Information Security Management Systems, Guidelines for Information Security Risk Management*. Norma de seguridad de la información publicada en 1995 por el British Standar Institute. En 1998, fue publicada la segunda parte. La primera parte es un conjunto de buenas prácticas para la gestión de la seguridad de la información –no es certificable– y la segunda parte especifica el sistema de gestión de seguridad de la información –es certificable–. La primera parte es el origen de ISO 17799 e ISO 27002 y la parte segunda de ISO 27001.

Backdoor: (Puerta trasera) Es un mecanismo mediante el cual se accede a una aplicación, servicio, o sistema por un método solo conocido por el desarrollador de la aplicación y habitualmente realizado en forma no autorizada.

Back Orifice: (BO) Una de las herramientas más antiguas y conocidas para el Hacking de Win 9X, originalmente diseñada como una herramienta de administración remota. Permite tomar el control de una máquina remota con la capacidad de enviar y recibir archivos, modificar registro, robar claves, etc.

BCP (Business Continuity Plan): Plan desarrollado para permitir que una organización pueda seguir con las principales operaciones de su negocio en caso de una contingencia o un desastre.

Bomba de correo: El envío masivo de grandes cantidades de correo electrónico para lograr que el sistema de la víctima colapse.

Tecnología de la información

Bomba Lógica: Código malicioso que se ejecuta cuando existen condiciones específicas para su activación. Esta técnica la utilizan muchos virus como mecanismo de activación. El famoso virus conocido como Martes 13, utilizaba esta técnica para activarse los martes 13.

Bots: Término utilizado en la primera internet derivado de la palabra "robot". Con él se denomina a pequeños trozos de software que tienen la finalidad de actuar de manera independiente en un computador, como un "robot" controlado remotamente por un atacante. Symantec reportó 6 millones de computadoras infectadas por bots en el segundo semestre del 2006.

C

Caja Ignífuga: Cofre apto para el resguardo de copias de seguridad (backup) específicamente desarrollado para la protección contra el fuego de medios magnéticos. Cerificados bajo Normas EN 1047 o UL-72

CISM: (Certified Information Systems Manager). Es una acreditación ofrecida por ISACA que certifica a profesionales de seguridad de información.

Cifrado: Proceso mediante el cual se codifica un mensaje en texto claro aplicándole un algoritmo matemático. De esta manera se genera un código ininteligible para quien no posea la clave que permite descifrar el contenido real.

COBIT: (Control Objectives for Information and related Technology) Asociación cuya misión es investigar, desarrollar, publicar y promover un conjunto de objetivos de control en tecnología de información con autoridad, actualizados, de carácter internacional y aceptados generalmente para el uso cotidiano de gerentes de empresas y auditores.

Código malicioso: Software capaz de realizar un proceso no autorizado sobre un sistema con un deliberado propósito de ser perjudicial. Virus, gusanos, troyanos son algunos ejemplos de código malintencionado.

Confidencialidad: Propiedad que garantiza que la información sea accesible solo a aquellas personas que están autorizadas para tener acceso a ella.

Contingencia: Corresponde a un hecho no previsto que interrumpe los servicios informáticos que soportan el negocio de una organización

Control: Conjunto de políticas, procedimientos, prácticas y estructuras organizativas que aseguran una garantía razonable o suficiente de que se lograrán los objetivos del negocio.

D

Delito: Acciones y omisiones dolosas y culpables penadas por la ley.

Denegación de servicio (DoS): Un ataque de este tipo desorganiza o niega completamente el servicio a usuarios legítimos, redes, sistemas u otros recursos por una saturación en la cantidad de solicitudes realizadas de forma maliciosa. Consumo de todo el ancho de banda de una red en particular. En 1996 un proveedor del servicio de internet (ISP) en el área de Nueva York, fue atacado durante una semana, negando el acceso a internet a más de 1000 compañías.

Desastre: Todo evento natural, accidental o intencional, repentino y no deseado, capaz de interrumpir la operación habitual durante el tiempo suficiente para afectar de manera significativa al negocio y que sobrepasa la capacidad de respuesta de la organización. Por lo general los desastres, por su magnitud pueden afectar a varias empresas de un sector.

Disponibilidad: Propiedad que garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con ella toda vez que se requiera, en el momento que se requiera y donde se requiera.

Dolo: Es la voluntad consciente, encaminada u orientada a la perpetración de un acto que la ley tipifica como delito

DRP: (Disaster Recovery Plan). Metodología que desarrolla los procesos necesarios para recuperar los servicios informáticos de una compañía en caso de una contingencia o un desastre.

E

EN 1047 (parte 1 y parte 2): Norma europea que establece la clasificación y los métodos para ensayo de la resistencia al fuego para cajas y sala ignífugas para la protección de hardware, medios magnéticos y otros medios porta datos.

Encriptación: Proceso de convertir datos de texto plano en texto cifrado mediante un algoritmo matemático para evitar que terceras personas lo puedan acceder.

Elevación de privilegios: Proceso mediante el cual el usuario engaña al sistema para que le otorgue derechos no autorizados, usualmente con el propósito de comprometer o destruir el sistema.

Enumeración: Proceso mediante el cual un atacante (hacker), una vez dentro de un sistema, intenta identificar cuentas de usuario válidas o recursos compartidos mal protegidos. Con esta información sólo es cuestión de tiempo el descubrir las contraseñas que le darán acceso al sistema.

Exploit: Falla de seguridad en el desarrollo de una aplicación o sistema que permite a un atacante penetrar al sistema y robar información.

F

Fireproof Vault: Sala preparada para el gerenciamiento de riesgos múltiples como fuego, calor, inundación, radiaciones electromagnéticas, acceso no autorizado, robo, vandalismo, terremotos, etc. (Ver Sala Cofre). Cumplimenta los requerimientos de protección de la Norma TIA 942.

Firewall: Aplicación o herramienta de hardware o software que funciona como sistema de defensa, para evitar cualquier tipo de acceso no autorizado a un determinado sistema. Estos programas suelen usarse para la protección de una computadora que está conectada a una red, especialmente internet. Controlan todo el tráfico de entrada y de salida, informando o evitando actividades sospechosas.

Firma digital: La firma digital consiste en la utilización de un método de encriptación llamado asimétrico o de clave pública. Este método consiste en establecer un par de claves asociadas a un sujeto; una pública, conocida por todos los sujetos intervinientes en el sector, y otra privada, sólo conocida por el sujeto en cuestión. De esta forma cuando se desea establecer una comunicación segura con otra parte basta con encriptar el mensaje con la clave pública del sujeto para que a su recepción sólo el sujeto que posee la clave privada pueda leerlo. Permite autenticar la identidad del usuario emisor y la propiedad de un documento en circulación.

Fallo de seguridad: Programa o técnica que aprovecha una vulnerabilidad del software. Los fallos de seguridad pueden utilizarse para provocar brechas de seguridad o atacar una red por otros medios.

G

Gestión del riesgo: Proceso de identificación, control y mitigación o eliminación, a costo aceptable, de los riesgos que afecten a los sistemas de información de la organización.

Gusano: Programa informático que se autoduplica y autopropaga. En contraste con los virus, los gusanos suelen estar especialmente escritos para redes. El primer gusano famoso de internet apareció en noviembre de 1988 y se propagó por sí solo a más de 6.000 sistemas a lo largo de internet.

H

Hacker: Persona que, gracias a sus grandes conocimientos en programación, informática y electrónica, tiene la capacidad para introducirse, salteando las barreras de seguridad, en redes o sis-

temas informáticos de particulares, empresas o instituciones que si están conectados a internet.

Honeypot: Son, en su forma más básica, servidores de información falsos, posicionados estratégicamente en una red de prueba, y alimentados con información falsa que es disfrazada como archivos de naturaleza confidencial haciéndolos altamente atractivos para un hacker en busca de un blanco. Por último, el servidor es habilitado con herramientas de monitoreo y rastreo de información, de manera que cada paso y rastro de actividad de un hacker pueda ser analizado y estudiado a fin de desarrollar medidas defensivas.

Hoax: Mensaje de correo electrónico inofensivo creado para su reenvío masivo que intenta hacer creer al receptor algo que es falso. Alertan especialmente sobre virus inexistentes y se difunden por la red, a veces con mucho éxito causando al final casi tanto daño como si se tratase de un virus real.

I

Impacto: El costo para la empresa de un incidente que puede o no ser medido en términos estrictamente económicos (pérdida de reputación, imagen, implicaciones legales, etc).

Integridad: Propiedad que salvaguarda la exactitud y totalidad de la información y sus métodos de procesamiento y comunicación. Debe contener en forma completa lo que se espera que contenga. También implica que la información que se recibe en un punto remoto de una red debe ser exactamente igual a la que se emitió en un punto local.

Ingeniería social: Es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Es habitual el uso del teléfono o internet para engañar a la gente y llevarla a revelar información sensible, o bien a violar las políticas de seguridad típicas. Con este método, los atacantes se aprovechan la tendencia natural de la gente a confiar en su palabra, antes que aprovechar agujeros de seguridad en los sistemas informáticos. Generalmente se está de acuerdo en que "los usuarios son el eslabón débil" en seguridad; éste es el principio por el que se rige la ingeniería social.

Inventario de activos: Detalle de los recursos físicos, información, software, documentos, servicios, personas, etc. que tienen valor para la compañía y necesitan ser protegidos de riesgos potenciales.

ISACA: (Information Systems Audit and Control Association). Asociación internacional de profesionales de la Seguridad de la Información, dedicados a la auditoria, control y seguridad de sistemas de información.

ISO 17799: (Código de Práctica para la administración de la Seguridad de la Información). Estándar internacional de seguridad que provee las mejores prácticas para la definición de controles proporcionando proactivamente soluciones para evitar interrupciones en las actividades y procesos del negocio, asegurando una protección adecuada para los sistemas de información contra amenazas internas y externas.

K

Kevin Mitnick: El hacker más famoso de todos los tiempos. Tras ser detenido en 1995 por el FBI, que lo acusaba de introducirse en los sistemas informáticos de empresas como Digital Equipment, Motorola Inc., Novell Inc., Nokia Corp. y Sun Microsystems fue condenado a 46 meses de prisión. Adicional a la sentencia el fiscal obtuvo una orden de la corte que prohibía a Mitnick el uso del teléfono en la prisión alegando que el prisionero podría obtener acceso a las computadoras a través de cualquier teléfono.

Keylogger: Programa que intercepta todas las pulsaciones realizadas en el teclado para obtener datos sensibles como contraseñas, etc. Las pulsaciones son guardadas a manera de archivos y posteriormente pueden ser enviados por mail a un tercero sin conocimiento ni consentimiento del usuario.

L

Lammer: Personas aficionadas, sin conocimientos avanzados de computación, que quieren hacerse pasar por hackers utilizando herramientas de dominio público.

N

NFPA: (National Fire Protection Association) Organización reconocida internacionalmente como la máxima autoridad fuente de conocimientos técnicos, datos, y mejores prácticas sobre la problemática del fuego orientada a la protección y prevención. Prácticamente cada edificio, proceso, servicio, diseño e instalación en la sociedad de hoy día, se ve afectado por los documentos (códigos y normas) de la NFPA.

NFPA 75: (Standard for the Protection of Electronic Computer/Data Processing Equipment). Estándar para la protección de Equipamiento de Procesos de datos y computadores.

No conformidad: Situación que evidencia el no cumplimiento de algún control, pudiendo atentar contra la confidencialidad, integridad o disponibilidad de información sensible, o bien representar un riesgo menor.

No repudio: Servicio de seguridad que evita que un emisor niegue haber remitido un mensaje, cuando realmente lo ha emitido, y que un receptor niegue su recepción, cuando realmente lo ha recibido.

P

Perito: Persona, que poseyendo la facultad y los conocimientos científicos, artísticos, técnicos, informa bajo juramento sobre puntos litigiosos la relación de su experiencia.

PGP: Pretty Good Privacy es el programa de cifrado por excelencia para la mayoría de usuarios que pretenden proteger su correo electrónico.

Phishing: Modalidad de estafa diseñada con la finalidad de robarle la identidad a usuarios de internet. El delito consiste en obtener información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños. Este tipo de fraude se recibe habitualmente a través de mensajes de correo electrónico. Para que estos mensajes parezcan aún más reales, el estafador suele incluir un vínculo falso que parece dirigir al sitio web legítimo, pero en realidad lleva a un sitio falso o incluso a una ventana emergente que tiene exactamente el mismo aspecto que el sitio web oficial. Estas copias se denominan "sitios Web piratas". Una vez que el usuario está en uno de estos sitios web, introduce información personal sin saber que se transmitirá directamente

al delincuente, quien la utilizará para realizar compras, solicitar una nueva tarjeta de crédito o robar su identidad.

Phreaking: Expertos en el hackeo de sistemas de telefonía fija o inalámbrica.

Política de seguridad: Documento que establece el compromiso de la dirección y el enfoque de la compañía en la gestión de la seguridad de la información.

Producto Listado: Según definición de NFPA *(Nacional Fire Protection Association)* es aquel producto o material, publicado en una lista por una organización idónea y autorizada técnicamente para la evaluación de productos y que mantiene evaluaciones periódicas para verificar el cumplimiento de los estándares y/o ensayos apropiados para que el producto pueda ser utilizado de la manera esperada. Estos listados son públicos y en la mayoría de los casos pueden ser consultados vía internet desde los sitios de los distintos organismos (UL, Omega Point Laboratories, Intertek, etc).

R

Red Privada Virtual (VPN): Red en la que al menos alguno de sus componentes utiliza la internet pero que funciona como una red privada, empleando para ello técnicas de cifrado que proporcionan un túnel a través del cual la información puede pasar de un nodo a otro de manera segura.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

S

Sala Cofre: Salas ignífugas conformadas como un cubo estanco de paredes, piso y techo a partir de paneles modulares que poseen compuestos aislantes que aseguran que la temperatura interior no superará los límites críticos del equipamiento informático en caso de un incendio. Preparadas para gerenciar riesgos múltiples alojan y protegen en su interior a un Centro de Procesamiento de Datos (CPD). Estas salas deben obedecer a la característica de Producto Listado (NFPA) y estar ensayadas de acuerdo a normas internacionales como UL-72 o EN 1047-2. Las Salas Cofre referidas como TIER 4 ofrecen hasta cuatro horas de Protección a 1.000 °C de temperatura.

Sniffer: Programa que busca una cadena numérica o de caracteres en los paquetes que atraviesan un nodo de la red con objeto de conseguir alguna información. Normalmente se usa con fines ilegales.

Sarbanes-Oxley: Ley de Reforma de la Contabilidad de Compañías Públicas y Protección de los Inversores aplicada en EE.UU. desde 2002. Se desarrolló teniendo como objetivo generar un marco de transparencia para las actividades y reportes financieros de las empresas que cotizan en Bolsa, y darle mayor certidumbre y confianza a inversionistas y al propio Estado. Se aplica a toda compañía registrada bajo el *Exchange Act* o que tiene una declaración de inscripción en espera bajo *Security Act*. Las multas por proveer información falsa o incorrecta son muy severas y pueden llegar al extremo de encarcelar a los ejecutivos de la empresa, o que ésta, sea retirada de la Bolsa de Valores en que cotiza.

SGSI: (Sistema de Gestión de la Seguridad de la Información). Sistema de gestión que establece, implementa, monitorea, revisa, mantiene y mejora la seguridad de la información, previo análisis de riesgos.

T

Ted Humphreys: Experto en seguridad de la información y gestión del riesgo, considerado "padre" de las normas BS 7799 y la ISO 17799 y, por tanto, de la ISO 27001.

TIA-942: (Telecommunication Infrastructure Standard for Data Centers). Norma internacional que establece los lineamientos a seguir en el diseño y planificación de un *Data Center* o *Computer Room.* Cubre las áreas de facility, arquitectura, energía, climatización, cableado y diseño de redes.

TIER: Clasificación definida por la norma TIA-942 en función de los niveles de redundancia y disponibilidad del Data Center. Establece cuatro niveles Tier 1, 2, 3 y 4.

Troyano: Programa que lleva oculta una funcionalidad determinada que será usada con fines maliciosos y en contra del usuario que lo instala. Se diferencia de los virus en que un troyano forma parte del código fuente del programa instalado y se compila junto con él, mientras que el virus simplemente se añade o suplanta al programa original. Hoy en día representan el 45% del código malicioso que circula por internet.

U

Underwriters Laboratories (UL): Laboratorio de ensayos referentes a seguridad fundado en 1894 y reconocido internacionalmente como la máxima autoridad en la materia.

UL-72: (Tests for Fire Resistance of Record Protection Equipment). Norma Americana (UL) que establece la clasificación y los métodos para ensayo de la resistencia al fuego para contenedores de hardware, medios magnéticos y otros medios porta datos.

V

Vinton Cerf: Científico norteamericano, nacido en 1943 y graduado en Ciencias de la Computación en 1956 en la Universidad de Stanford. Trabajó en la década del 70 en el desarrollo de la red de comunicaciones militares ARPANET y precursora del actual internet. Desarrolló junto a Robert Kahn el protocolo TCP/IP y es considerado el "padre" de internet.

Virus: Programa cuyo objetivo es causar daños en un sistema informático y que a tal fin se oculta o disfraza para no ser detectado. Estos programas son de tipos muy diferentes y pueden causar problemas de diversa gravedad en los sistemas a los que infectan. Hoy se propagan fundamentalmente mediante el correo electrónico.

Vulnerabilidad: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo de la compañía.

Hay que tener en cuenta que todos los sistemas son vulnerables ya que dependen de la falibilidad de los desarrolladores que los programan y fundamentalmente de las posibles fallas falibilidad de las personas que los operan.

Es sabido que el eslabón más débil en la cadena de seguridad es el recurso humano y a el apuntan muchos de los controles a implementar abarcados por las mejores prácticas de todas las normas que se ocupan del tema.

El mundo global e interconectado de hoy hace que las amenazas se propaguen en tiempo real generando costos de miles de millones de dólares en concepto de indisponibilidad de sistemas, fraude económico y robo de información en beneficio de terceros. Sólo hay que tomar los recaudos necesarios e implementar las políticas de seguridad existentes a fin de minimizar los riesgos dentro de una ecuación costo-beneficio aceptable en función de la magnitud y el negocio de las compañías. ■