UNIDAD 4

FALLOS EN LA SEGURIDAD INFORMATICA

1.4 INTRODUCCION

Dentro la amplia variedad de amenazas que afectan a los equipos informáticos siempre se cristalizan en una única consecuencia: el sistema deja de funcionar.

El fallo determina la paralización del sistema puede conllevar otro impacto aún mayor: la destrucción o desaparición de la información almacenada, que muchas veces es casi imposible de recuperar, o lo es con unos costos muy elevados, entre los diversos riesgos podemos examinar los siguientes que detallamos:

1.4.1 Clasificación de las amenazas

De forma general podemos agrupar las amenazas en:

- Amenazas físicas
- Amenazas lógicas

Estas amenazas, tanto físicas como lógicas, son materializadas básicamente por:

- las personas
- programas específicos
- catástrofes naturales

Tambien podemos tener otros criterios de agrupación de las amenazas, como ser:

Origen de las amenazas

Amenazas naturales: inundación, incendio, tormenta, fallo eléctrico, explosión, etc...

Amenazas de agentes externos: virus informáticos, ataques de una organización criminal, sabotajes terroristas, disturbios y conflictos sociales, intrusos en la red, robos, estafas, etc...

Amenazas de agentes internos: empleados descuidados con una formación inadecuada o descontentos, errores en la utilización de las herramientas y recursos del sistema, etc.

Intencionalidad de las amenazas

- **Accidentes**: averías del hardware y fallos del software, incendio, inundación, etc...
- **Errores**: errores de utilización, de explotación, de ejecución de procedimientos, etc...
- **Actuaciones malintencionadas**: robos, fraudes, sabotajes, intentos de intrusión, etc...

Para un analisis específico, nos enfocaremos basicamente en las amenazas de tipo físico y lógicos, tal como se ha mencionado,

1.5 Fallos o Amenzas Físicas

1.5.1 Obsolescencia de los soportes de almacenamiento

La rápida evolución de las tecnologías de almacenamiento (tarjetas perforadas, cintas magnéticas, casetes, discos magnéticos, discos compactos, etc.) implica que, al pasar el tiempo, la información grabada en un determinado soporte sea prácticamente irrecuperable al no disponerse de los periféricos de lectura adecuados. El trasvase de ingentes cantidades de información de un tipo de soporte a otro implica una gran cantidad de tiempo de sistema y elevados costes económicos, por lo que muchas veces no se hace.

1.5.2 Amenazas naturales

Las instalaciones de procesos de datos se encuentran sometidas a todo tipo de amenazas y catástrofes (terremotos, riadas, tormentas, incendios, etc.) que pueden provocar la interrupción del funcionamiento y, en muchos casos, la destrucción del sistema. Las estadísticas indican que un elevado número de empresas u organizaciones que han tenido un incidente de seguridad de este tipo han quebrado o desaparecido en un breve lapso de tiempo.

Medida de seguridad: equipo alternativo o plan de contingencia.

1.5.3 Problemas eléctricos y electromagnéticos

Los fallos del suministro eléctricos y las radiaciones electromagnéticas pueden alterar el funcionamiento de los equipos y los datos almacenados de forma magnética.

Medidas de seguridad: sistemas antifallo de alimentación continua y normativas de protección.

1.5.4 Sabotajes y actos terroristas

La concentración de la información y el control de numerosos sistemas, (tráfico aéreo, ferroviario, comunicaciones, sistemas energéticos, etc.) en los centros de proceso de datos los hace especialmente vulnerables a este tipo de actos que buscan paralizar la sociedad. Por lo tanto los CPD se convierten en objetivos de primer orden para grupos revolucionarios o terroristas. Recuérdese el atentado de ETA al centro de Informática de Telefónica en la calle Ríos Rosas o los 25 atentados efectuados por las Brigadas Rojas contra centros de interés estratégicos del Estado Italiano en los años 80.

Medidas de seguridad: las habituales de protección de edificios e instalaciones.

1.5.5 RIESGOS QUE AFECTAN A LOS SISTEMAS LÓGICOS

Este tipo de riesgo suele ser uno de los más peligrosos y difíciles de detectar, ya que al alterar el

funcionamiento normal del sistema y no detectarse a tiempo puede provocar daños irreparables a la información, a los usuarios e incluso al sistema físico.

1.5.6 Ciberplagas

A veces también se el denomina como software malintencionado. Abarca un conjunto diverso de programas (virus, gusanos, caballos de Troya, etc.) cuyos objetivos es adueñarse del control del sistema operativo con el fin de provocar, en la mayoría de los casos, la destrucción de la información u otros tipos de daños a los sistemas informáticos.

Las características de los principales tipos de software malintencionados son las que se explican en los siguientes párrafos, aunque lo normal es que no existan tipos puros, sino programas que reunen las características de varios de los tipo básicos.

Virus.

Son programas que modifican otros programas o alteran los ficheros. Antes se propagaban a través de programas en disquetes que al introducirse en los PC, se liberaban y realizaban sus comandos. Hoy día se propagan principalmente a través del correo electrónico, de ahí su gran poder de propagación debido al desarrollo de los e-mails. Se les denomina así debido a su parecido con los virus biológicos ya que necesitan para vivir un cuerpo vivo, el sistema informático y la red en funcionamiento, y además son capaces de reproducirse y de morir, mediante la utilización del software adecuado.

Hay dos tipos de virus. Los **benignos** y los **malignos**.

Los primeros sólo producen efectos molestos como la superposición de mensajes (el virus Marihuana) o movimiento de figuras (virus de la Pelotita) o transposición de los caracteres de la pantalla (virus de la cascada de letras).

Los malignos pueden borrar ficheros de datos o alterar el funcionamiento de los programas. Los más conocidos son Viernes 13, Melissa (creado por David L. Smith), Love Letter de Raonel Ramones, Back Orifice de Sir Dyistic, The Tour of de Worm de Morris, y el Chernobyl de Chen Ing-Hou. Hay que destacar que el primer virus de la historia fue construido por el investigador informático Fred Cohen cuando trabajaba en conseguir programas inteligentes que pudieran automodificarse, dando lugar a un rama de la informática, de inquietante futuro, la Informática Evolutiva o Vida Artificial.

Caballos de Troya o troyanos.

Son instrucciones introducidas en la secuencia de instrucciones de otros programas legales (de ahí su nombre) y que realizan funciones no autorizadas, destruyen ficheros o capturan información mientras simulan efectuar funciones correctas. Un caso particular de los troyanos son los salami, generalmente utilizados en instituciones financieras, realizan asientos de pequeñas cantidades, como los redondeos de operaciones de cálculo de intereses, par que no se detecten por su importancia y al final se transfieren a una cuenta bancaria particular.

Bombas lógicas.

Son programas que se activan en determinadas condiciones tales como una fecha determinada (Viernes y 13) o la presencia o ausencia de un determinado dato en un fichero. Se ha detectado que su uso más común es como elemento de venganza de algún empleado. Caso típico es la bomba que se activa cuando un determinado empleado, su autor, no aparece en el fichero de nómina, por haber sido despedido. El efecto de una bomba es libera un virus o un troyano. Una bomba lógica puede estar inactiva durante años.

Remailers

Son programas relacionados con la administración y gestión del correo electrónico, que pueden generar órdenes de envío de correos desde un origen a diversos destinatarios y a su vez, utilizando su libreta de direcciones, reenviarlos a estos nuevos destinatarios, creando una cadena de envíos. Actualmente es la manera más común de propagar virus. Johan Helsingius fue el primer conductor de un remailer anónimo

Electronic Mail Bombs

Son también programas relacionados con el correo electrónico y permiten generar órdenes de envío de correos desde uno o varios orígenes a un solo destinatario, generándole una gran cantidad de órdenes y mensajes, con el fin de bloquear su funcionamiento e impidiéndoles, por ejemplo, atender pedidos o responder consultas. A este efecto se le conoce como denegación de servicios.

Worms o gusanos

Deben a su origen a los investigadores Robert Thomas Morris, Douglas McIlroy y Victor Vysottsky, desarrolladores de un juego de estrategia denominado Corewar (Guerra de la Memoria), que consistía en que ganaba el jugador que era capaz de ocupar más cantidad de memoria. El gusano no necesita, a diferencia de los virus otro programa para funcionar y simplemente se va duplicando y ocupando memoria hasta que su tamaño desborda al sistema informático en que se instala, impidiéndole realizar ningún trabajo efectivo.

Recuperadores de elementos borrados

Cuando se da la orden de borrar un Fichero, ya sea de datos o de programas, realmente lo que se hace es declarar, en el directorio que controla el soporte, que el espacio que antes estaba ocupado queda libre para almacenar otra información. Por consiguiente, la información antigua permanece en ese lugar, no se ha borrado físicamente, pero es inabordable por los sistemas normales. La información sólo desaparece cuando otra ocupa su lugar. Los programas recuperadores permiten obtener esa información siempre que no se haya superpuesto otra; de esta manera se obtiene informaciones teóricamente destruidas. El ejemplo más conocido es el del teniente coronel Oliver North.

Puertas falsas o Back Doors

Está técnica permite introducirse en los programas por puntos que no son los estándares o normales. En principio eran utilizados por los programadores para facilitar el proceso de pruebas, evitando tener que procesar todo el programa o sistema para probar sólo un trozo. Si estas puertas falsas se mantienen en la versión operativa, bien de forma intencionada o por descuido, se crean agujeros en

la seguridad de la aplicación.

Sniffers o Rastreadores

Son programas que se ejecutan en una red informática y rastrean todas las transacciones que viajan por ella para volcarlas en un fichero. El estudio de este fichero permite encontrar claves, passwords o números de tarjetas de crédito, que pueden ser utilizados de forma fraudulenta. En general los programas están escritos en lenguaje C y pueden encontrarse disponibles en algunos foros de debate de Internet.

Medidas de seguridad: antivirus y cortafuegos (firewalls) y otros tipos de software de protección y de rastreo de cadenas de bits identificables como de operaciones peligrosas y programas de análisis del log del sistema para detectar transacciones no autorizadas.

1.5.7 Copias ilegales

Cada vez más circulan por la red todo tipo de programas que permiten la copia de otros programas, música, tarjetas de TV, CD, películas, etc. Todo ello ocasiona un fraude a los derechos de autor y a los beneficios de empresas editoras, cinematográficas, discográficas, de TV, etc., que se elevan a miles de millones anuales, y que ponen en peligro el futuro de algunos sectores económicos dedicados al ocio.

En una comparación en Europa, España es uno de los países que se encuentra a la cabeza en el ranking de la piratería informática. Solamente un ordenador situado en una Universidad de un país centroamericano realizaba copias maestras de CD y tras un pago muy inferior a su valor de mercado y a través de otros equipos distribuidores ubicados en el Reino Unido, Alemania y España, distribuía sólo en España 100 CDs diarios de software ilegal provocando unas pérdidas de unos 4.000 millones de pesetas. El monto es mucho más importante en el caso de los CD musicales y juegos de Ordenador.

En latinoamerica, el indice de pirateria se disputa entre Perú y Bolivia

Medidas de protección: Cambio periódico de los sistemas de protección de los diferentes soporte. Estas medidas son muy poco eficaces, ya que en plazos muy breves aparecen sistemas de desprotección.

1.5.8 Denegación de servicios

Consiste en el envío de mensajes masivos a un servidor, mediante los programas ya comentados, con el único fin de saturarlo y bloquearlo, impidiendo el normal funcionamiento del sistema.

El riesgo es muy importante en servidores y hosts que administran servicios importantes como el tráfico aéreo, ferroviario, distribución eléctrica, o seguridad nacional por las graves consecuencias que para el normal funcionamiento de los correspondientes servicios tendría la denegación de los mismos.

Medidas de protección: Separar el servidor de correo electrónico o de páginas web de la red local o de la Intranet del usuario. Muchas veces esto es imposible por la propia configuración del sistema. Además en los entornos de la Seguridad Informática, existe el aforismo de que el único ordenador seguro es el que se encuentra aislado en una habitación con las correspondiente medidas de seguridad física y sin estar conectado a ninguna fuente de suministro eléctrico. Es decir, un ordenador inactivo, muerto.

1.6 OTROS RIESGOS QUE AFECTAN A LA INFORMACIÓN

La información es el elemento más sensible de todo el sistema informático, por lo que conlleva el riesgo de accesos no autorizados, que utilicen esa información o que la modifiquen, lo que puede ser mucho más grave.

Para proteger la información, tanto en su almacenamiento como en su transmisión, se debe emplear métodos criptográficos o de cifrado que dificultan el conocimiento del contenido real.

1.6.1 Captura de emisiones electromagnéticas

Todos los equipos informáticos, y especialmente las pantallas, generan radiaciones electromagnéticas que pueden ser captadas con los equipos apropiados situados a la distancia conveniente, por ejemplo, en una furgoneta en la calle.

Medidas de seguridad: Aplicar la normativa Tempest y cristales apropiados en las ventanas.

1.6.2 Interceptación de líneas de datos

Las líneas de datos pueden ser interceptadas, lo que permite la captura de toda la información que fluye por ellas.

Actualmente muchas de los métodos de transmisión son inalámbricos, viajando las información a través del éter y utilizando satélites de comunicaciones, por lo que la línea no es segura y la información tanto digital como analógica puede ser captada, almacenada y posteriormente analizada.

Entre los ejemplos reales se considra la existencia de la red ECHELON, tanta veces negada por los EEUU y Gran Bretaña, es una prueba evidente de este peligro, ya que algunas veces la información obtenida ha sido utilizada para el espionaje industrial y no sólo para la lucha contra el crimen organizado y el terrorismo internacional.

Medidas de seguridad: Uso de canales seguros y cifrado de la información transmitida mediante criptografía.

Acceso no autorizado a las bases de datos

El acceso no autorizado a las bases de datos tiene como objeto obtener la información almacenada (espionaje, fraude monetario o comercial, chantaje, etc) o cambiar esa información (sabotaje, terrorismo, fraude, etc.), éste suele ser el objetivo principal de hackers y crackers.

Medidas de Seguridad: Sistemas sofisticados de gestión de claves de acceso y cifrado de la información residente en las bases de datos.

1.7 RIESGOS ASOCIADOS A LAS PERSONAS

El mal uso de los sistemas de información y de Internet por personas malintencionadas pueden generar problemas de todo tipo Agrupamos en este apartado un diverso conjunto de riesgos que van desde los delitos o transgresiones a los Códigos Civil y Penal (los mal llamados delitos informáticos, ya que sólo utilizan la informática como instrumento para el delito) a problemas de tipo psicológico.

1.7.1 Hackers y cracker

Las noticias de la prensa (un hacker entra en el ordenador de la Moncloa o del Pentágono), películas (Juegos de Guerra) o novelas (La piel del tambor) nos habla de este fenómeno ligado a Internet: el acceso no autorizado a un sistema informático y el control de la administración del mismo por un extraño.

Los organismos que se dedican a registrar los incidentes de ataques a sistemas detectan un incremento continuo de esta actividad, que si en algunos casos no causa daño, siempre provoca molestias y dudas, ya que a nadie le gusta que entren en su casa sin ser invitado y curioseé en sus propiedades y hurgue en sus intimidades. En el primer semestre del año 2002 se han denunciado y registrado una cantidad de ataques superior a la de todo el año 2001.

Se discute que si los hackers son buenos y los crackers delincuentes. En los foros hackers, y hay muchos en la red, pueden encontrarse su justificación. Para ellos, la motivación principal de un hacker es la curiosidad para perfeccionarse en el conocimiento informática mediante la práctica, utilizando los medios adecuados, no importa cuáles. Su definición de hackers es una persona que posee conocimientos avanzados sobre una materia

En concreto, normalmente relacionada con la tecnología y que los pone al servicio de un único objetivo: **EL CONOCIMIENTO**. Desean conocer como funcionan las cosas y con el único límite de su propia curiosidad. No se dedican a destruir y causar daños a sus "víctimas", y suelen advertir a terceros de las debilidades de sus sistemas. En cuanto pasan a beneficiarse mediante fraudes u otras ilegalidades o a causar estragos en los sistemas atacados, traspasan la frontera y se convierten en crackers.

De hecho, los profesionales de la auditoría informática de seguridad utilizan en su trabjo las mismas herramientas de los hackers para probar la seguridad de los sistemas a estudio, atacándolos para descubrir sus vulnerabilidades. Muchas de estas herramientas, como SATAN, se encuentran a disposición de todo el mundo y libre de costos en la red.

Los amplios conocimientos adquiridos por los hackers en su actividad, los hacen muy cotizados por Gobiernos y empresas para contratarlos como asesores de seguridad, ya que una ética, mal entendida, hace que los estudios de este tipo no suelan impartirse en las Universidades, con el resultado de una fuerte carencia de profesionales de la Seguridad Informática.

Medidas de seguridad: Auditorías del sistema para determinar las debilidades del mismo y posibles puertas falsas de entrada.

1.7.2 Relaciones sindicales.

La Red ha incorporado una nueva forma de trabajar: el teletrabajo. El trabajador ya no necesita desplazarse para realizar su actividad, puede trabajar a distancia. Pero independientemente de las ventajas (más tiempo de ocio, menos tráfico, entorno de trabajo a medida, menos inversión en locales y gastos generales) e inconvenientes (falta del grupo y de las relaciones interpersonales, cesión de parte del domicilio particular a la empresa, nuevo tipo de relación laboral y de contrato, generalmente un sueldo más bajo) que esta nueva forma de relación laboral aporta a trabajadores y empresas, surge una pregunta: ¿qué pasa con los sindicatos?, ¿cuál es su papel en esta nueva economía?,.

Al fragmentarse el entorno e individualizarse las relaciones laborales se altera el comportamiento sindical tradicional al fomentarse las relaciones informales, la autodisciplina y la desaparición de la jerarquía formal. Aunque las organizaciones sindicales puedan utilizar la red para extenderse y apoyar sus reivindicaciones es difícil organizar "piquetes informativos virtuales" que persuadan a sumarse a los trabajadores a una huelga en el ciberespacio. Además el trabajador tiende a hacerse más autónomo y en autoempleadores o trabajadores para más de un empresario. La desaparición o pérdida de poder de las organizaciones sindicales puede redundar en una pérdida de derecho para los trabajadores.

Blanqueo de capitales

Es posible encontrar en Internet páginas WEB que facilitan esta operación mediante la compra de bienes de importancia (empresas, terrenos o inmuebles) generalmente en paraísos fiscales. La operación se avala por bancos que realizan transferencia bancarías incluso con datos falsos; lo importante es la transferencia, no el origen del dinero, ni el remitente.

En muchos casos el dinero procede de actividades ilícitas (tráfico de drogas o armas, fraudes electrónicos, etc.). El uso de Internet en este delito clásico favorece esta actividad, ya que la operación se efectúa a través de ordenadores manteniendo el anonimato de la persona que realiza la transferencia.

Ciberterrorismo

Los grupos terroristas cada vez actúan más como grupos organizados con diversos frente de ataque como el de la propaganda, la captación de adeptos o desinformación. Así mientras la embajada del Japón en Lima, en la Navidad de 1996, se encontraba ocupada por guerrilleros, otros militantes del Movimiento Revolucionario Tupac Amaru luchaban en el ciberespacio poniendo decenas de páginas de la web con propaganda guerrillera. Lo mismo sucede con las FARC, el EZLN o ETA.

Pero algunos de los riesgos ya presentados, como el ataque a sistemas, la denegación de servicios o la manipulación de la información, pueden convertir a Internet en la puerta trasera del terrorismo internacional.

Por otro lado, dentro de la Administración Busch en Estados Unidos, presentó el día 18 de Septiembre de 2002 el borrador de un plan de acción, dotado de 4.300 millones de dólares, para restringir el acceso a las redes informáticas federales. El documento Estrategia Nacional para la Seguridad en el

Ciberespacio, incluye 60 recomendaciones a los usuario de la red, tanto particulares como empresariales. El plan no es definitivo ya que, al no haberse consultado a los usuarios, ha provocado las protestas de la industria informática por el coste que la incorporación de las medidas de seguridad en sus productos software. Se ha abierto un período de alegaciones de dos meses.

Uno de los planes es la creación de un gran centro de control nacional que detecte de forma preventiva cualquier actividad informática sospechosa, lo que provoca sospechas en los defensores de los derechos civiles.

1.7.3 Pornografía y pornografía infantil

Actualmente es uno de los negocios que proporcionan más dinero en la red y el de la pornografía infantil de los más perseguidos en todo el mundo. Como otros delitos, ya se realizaban antes, pero la red ha permitido su expansión y dificultado la identificación y localización de los responsables.

Y el problema principal, de todas formas, es como pueden proteger los padres a sus hijos de los pedófilos que merodean por la red y como pueden limitar el acceso a sus páginas o a otras de contenido violento, racistas o sectarias. La prohibición total no es la solución y la red no puede distinguir entre adultos y niños.

Apologías de grupos violentos o partidos ilegales

Al igual que los grupos terroristas, los gobiernos, las organizaciones, las universidades y las empresas utilizan la red para dar información, servicio, promocionarse y obtener afiliados y clientes, cualquier persona o grupo puede instalar una página en cualquier servidor situado en países cuya legislación sea más permisiva. Lo mismo que existen paraísos fiscales existen paraísos cibernéticos; lo que dificulta la lucha contra estas apologías de la violencia, del racismo, del sexismo o de sectas pseudo-religiosas. La implantación de una legislación sobre Internet en todo el mundo y de forma consensuada parece en estos momentos un objetivo inalcanzable.

Pérdidas de la intimidad

Las sociedades occidentales suelen estar muy celosas de su intimidad. La mayoría de las personas se preocupan del mal uso que pueda hacerse de sus datos. El miedo a un mundo orwelliano, al Gran Hermano cibernético es real. Por ello muchos países han promulgado leyes de protección de los datos de carácter personal, como es el caso de España. Con la LORTAD y su sucesora la LOPD.

Pero la situación después de los atentados del 11-S la situación ha cambiado drásticamente y directivas y legislaciones europeas y nacionales tienden, en nombre de la seguridad, a recortar derechos y a imponer obligaciones extras a las empresas del mundo cibernético.

La tendencia a obligar a los operadores de servicios de Internet, los registros de transacciones durante un período de tiempo más o menos largo, obliga a un incremento de los soportes de información y a unos costes de mantenimiento muy elevados.

La existencia de estos “Grandes Hermanos” hace pensar en que es necesario incrementar los controles democráticos sobre los gobiernos para defender el uso y disfrute de los derechos de intimidad.

1.7.4 Desinformación y unificación cultural

La red se ha convertido en un aula inmensa a la que pueden acceder personas de toda edad y nivel cultural, lo cuál facilita no sólo la educación sino también la formación permanente. Pero al mismo tiempo divide a la humanidad en dos grandes grupos: los conectados y los que no tienen acceso a la red, por lo que las consecuencias pueden ser el incremento de las diferencias entre ambos mundos.

Por otra parte, hoy día, todo lo que no se encuentra en la red no existe; lo que significa un peligro para muchas lenguas y culturas. Habrá que hacer un gran esfuerzo cultural y económico para evitar la pérdida de este patrimonio de la Humanidad.

Además el monopolio de las inversiones de las grandes compañías de informática en los contenidos de la red provocan una globalización (para muchos autores americana) de la información y de la cultura

1.7.5 Las comunicaciones de crimen organizado

Desde la más remota antigüedad las comunicaciones y las informaciones sensibles se han cifrado para su protección. Durante siglos, hasta la aparición de los computadores, la Criptografía ha sido prácticamente un arte. La potencia de cálculo de los computadores y el desarrollo de nuevos y potentes algoritmos de cifrado han facilitado la protección informática de la información que circula por la red y se almacena en sus servidores.

Este cifrado de la información cuando es utilizado por organizaciones criminales dificultan la labor de jueces y policías. aunque se intercepten legalmente las comunicaciones. El trabajo de descifrado mediante computador sin conocer la clave utilizada puede requerir cientos de años.

Las iniciativas que intentaban obligar a almacenar las claves en un depositario y cuyo acceso estaba restringido al poder judicial (clipper chip) no han prosperado.

1.7.6 Fraude electrónico

Es típico del comercio electrónico. El problema con que se encuentra un usuario de la red, atraído por una oferta de una web, es saber quién es el oferente, si va a cumplir, si va a recibir el producto, el poner los datos de su tarjeta de crédito en la red.

Las legislaciones europeas intentan resolver este problema regulando la llamada firma digital, que es un documento electrónico que hace el papel de acta notarial o contrato, avalado por un certificador o notario electrónico.

También existen programas informáticos que generan aleatoriamente números de tarjetas o claves de acceso y que cuando comprueban la coincidencia con alguna real, las utilizan para un uso ilícito