LA SEGURIDAD DE LA INFORMACIÓN EN LAS EMPRESAS

Daniel Eduardo Acosta Velázquez

djdanie1@hotmail.com

Eloy Negrete Hoz

negrete.oz@hotmail.com

Estudiantes de la Licenciatura de Informática.

"El arte de la guerra nos enseña a confiar no en la posibilidad de que el enemigo no venga. Sino en nuestra propia disponibilidad de recibirlo; no en la disponibilidad de que no ataque, sino en el hecho que hemos logrado que nuestra posición se inexpugnable"

El arte de la guerra, SUN TZU

Resumen:

En este articulo conocerán las formas en que los piratas informáticos utilizan su sabiduría en la informática y aprovechan para cometer delitos empezando por la piratería y que puede llegar hasta los virus para poder extraer información confidencial de una empresa a tal grado que las empresas se pueden ir ala quiebra o incluso extraer la información de un usuario promedio desde sus contactos hasta números de tarjetas de crédito. Debe tener en cuenta que al menor síntoma que presente su ordenador de algún virus deberá llamar a un técnico para que se encargue de eliminar cualquier amenaza y si ya esta siendo victima de robo de información deberá reportarlo con las autoridades correspondientes.

Palabras claves: Seguridad, información, empresas, delitos, informática, piratas informáticos, computadora.

Summary:

In this article we will learn about the ways in which hackers use their knowledge in computers to commit crimes and take advantage of starting with piracy and viruses can be up to extract confidential information from one company to the extent that companies can go wing bankruptcy or even extract information from an average user from your Contacts to credit card numbers. You should be aware that the slightest symptom submits its computer viruses should call a technician to take care to remove any threat and if it is being a victim of data theft should be reported to the authorities.

Keywords: Security, information, business, crime, computer hackers, computer.

1. Introducción

Las amenazas de las empresas aumentan constantemente y de diferentes tipos. El campo en la seguridad informática es muy amplio. Se puede definir como: “La protección contra todos los daños sufridos o causados por la herramienta informática y originados por el acto voluntario y de mala fe de un individuo”. La protección de un sistema informático en una empresa consiste en poner un alto contra las amenazas potenciales. Dado que ninguna protección es infalible, se requiere aumentar las barreras sucesivas. Así cualquier amenaza por parte de un pirata informático se vería bloqueada. También es necesario proteger todos los medios de acceso a la empresa, muy seguido vemos empresa sobreproteger su conexión de internet dejando otras vías de acceso abiertas y sin protección. Es necesario implementar las principales medidas (cortafuegos, antivirus, sistema de cifrado VPN, etc.) que sin duda alguna aportara un buen nivel de seguridad. [1]

En este artículo se analiza con detalle las potenciales amenazas a la seguridad en la empresa y las diferentes medidas que se deben tomar contra ellas. La sección 2 habla sobre el pirateo es decir el acceso no autorizado de un pirata informático a todo o parte del sistema de información de la empresa. La sección 3 explica la denegación de servicio (en ingles: Denial of Service DoS) donde en atacante no obtiene un acceso al sistema informático de la empresa, donde puede realizar estragos en los componentes estratégicos (el servidor de correo, el sitio web, etc.). En la sección 4 se toca el tema de los virus y sus diferentes tipos (gusanos, backdoor, caballo de troya), consisten en programas maliciosos, que se reproducen de manera más o menos autónoma. En la sección 5 trata sobre la intercepción de datos confidenciales, no dañan directamente los sistemas informáticos, una persona ajena a la empresa que pudiera obtener datos de forma indebida o documentos confidenciales podría causar un gran daño a la empresa. Finalmente en la sección 6 se presentaran una solución a los principales problemas que amenazan la seguridad en las empresas. [2]

2. Piratería en la información

La piratería informática es la distribución o la reproducción ilegal de fuentes o aplicaciones de software utilizadas para su uso comercial o personal. Ya sea deliberada o no la piratería informática es ilegal y esta castigada por la ley. Hoy

---

[1] Royer, Jean-Marc, Seguridad en la informática de empresa, (Barcelona, Ediciones ENI, 2004), pág. 9

[2] *Ibíd.*

en día existen poderosos antivirus que puede proteger su equipo contra errores potenciales, fallos del sistema y virus que pueden incluirse dentro del software pirateado. Existe una gran variedad de tipos de piratería entre los más comunes son: Usuario Final, en Internet, Carga en el Disco Duro y Falsificación de Software. A continuación se describen estos tipos de piratería. Es fácil ser victima de piratería de un usuario final un ejemplo muy común de abuso de usuario final se produce cuando empleados de una empresa realizan copias de software o comparten CD de instalación sin comprar nuevas licencias que sin las licencias adecuadas no podrá recibir soporte técnico ni actualizaciones. [3]

Figura 1 Piratería de la Información. Diversos Tipos de Piratería (Creación Propia)

En internet hay muchos sitios que venden productos piratas hacen creer a los usuarios que los productos que venden son originales poniendo anuncios que están en venta de liquidación por inventario etc. También hay muchos sitios de subastas que ofrecen software pirata o falso por ello no es recomendable descargar antivirus o cualquier otro programa de sitios desconocidos por que es probable que el software sea defectuoso o contenga virus o aplicaciones espía. Cuando los vendedores ofrecen ordenadores nuevos cargan copias ilegales de software o productos sin licencia se le conoce como carga en el disco duro, por eso se debe evitar las cargas de software ilegal cuando se desarrollan e implementan sistemas empresariales en algún lugar de trabajo. Los falsificadores de software copian y venden productos protegidos por copyright de manera ilegal a usuarios que desconocen el mundo de la informática y que no sospechan que el software que esta comprando sea

[3] Aceituno, Vicente, Seguridad de la Información, (Creaciones Copyright, 2004) pág. 12.

pirata. Es muy difícil identificar software pirata por que incluyen embalajes muy sofisticados, manuales y tarjetas de registro.

Es muy común que los usuarios se den cuenta de que su producto es pirata cuando lo quieren registrar y no pueden y por lo tanto no funcionara correctamente.[4]

Algunas recomendaciones que debemos de tomar en cuenta es que cuando compremos productos en línea es necesario asegurarnos de que el vendedor muestre alguna imagen del producto que vallamos a compra, evitar entrar en sitios de subastas en línea por que es muy probable de que seamos victimas de piratería y comprar los productos solo con distribuidores autorizados para asegurarnos de que el producto sea original. Hay también otros riesgos asociados a la piratería como son el Pishing y Spoofing y el mensaje de correo electrónico no solicitado mejor conocido como “Spam”. El “pishing” es la practica ilegal que consiste en engañar a los clientes para que estos proporcionen su información personal para después utilizarla para robar la identidad así como otras actividades ilícitas. El “spoofing” es algo parecido en el robo de identidad en el “pishing”. Aunque el “spam” es fácil de detectar el de tipo “spoofing” es mucho más engañoso. Estos correos parece que proceden de alguna empresa que pudiera ser con alguna que el usuario tenga relación y lo redirige a una pagina donde pide que el usuario proporcione información personal como: nombre, dirección, numero de cuenta bancaria y algún otro dato que les pueda servir a los piratas informáticos para que puedan utilizar cualquier tipo de información que el usuario introduzca.[5]

Para evitar el robo de identidad siempre que reciba un correo electrónico que le pida que proporcione su información primero debe contactar ala empresa que se lo manda, nunca confiar en el número telefónico que aparece en el correo electrónico y nunca proporcionar su información personal a petición de algún correo electrónico no solicitado, aunque el sitio al que lo guie parezca autentico. Para detectar los correos electrónicos no solicitados tipo “spoofing” contiene muy a menudo un saludo más genérico de lo que se espera de una empresa de la cual ya tiene información personal sobre el usuario. Estos tipos de correo electrónicos pueden dirigir a sitios web falsos que están diseñados para parecer auténticos pero que en realidad los usan para recabar información y utilizarlo de manera ilegal. Además de los enlaces a páginas web falsas algunos correos electrónicos te dirigen a sitios web legítimos.[6]

---

[4] *Ibíd.*
[5] *Ibid.*
[6] *Ibid.*

Los usurpadores de identidad lo hacen para que el correo falso parezca autentico. Aun así nunca proporcione su información personal a petición de algún correo electrónico no solicitado por que ninguna empresa en la actualidad usaría este medio.[7]

En conclusión es importante que todas las personas que están involucradas en el mundo de la informática conozcan todas las amenazas y riesgos que existen en internet ya que podría ser victima de los piratas informáticos. Es por ello que deben evitar los tipos de pirateo descritos previamente y navegar de una forma segura en las paginas web.[8]

3. Ataques DoS (Denial of Service)

El ataque DoS (Denial of Service) tiene como objetivo principal sacar de servicio las maquinas del objetivo fijado, con esto se busca que se deje de brindar el servicio que se ofrece. Hay dos tipos de efectos que el ataque DoS ocasiona, uno de ellos es dejas de brindar un servicio, hasta el paro total en el servicio operativo de la maquina afectada. Los ataques DoS son muy peligrosos resultan relativamente simples de hacer, para esto no se necesita tener una gran conocimiento sobre este tema, ni prescindir de grandes maquinas para llevar acabo la denegación del servicio. Todo aquel que quiera perjudicar a una empresa solo necesita de una conexión de internet para realizarlo y una de los tantos tipos de herramientas que se encuentran en internet todas ellas gratuitas y de fácil utilización. El mayor problema que tendría la empresa al recibir este tipo de ataque seria una gran perdida económica. Difiriendo mucho de un ataque buffer overflow que pertenece a otro tipo de realizado por los piratas informáticos, que no representa una gran amenaza, la denegación de servicio solo tiene como objetivo el dejar fuera de funcionamiento las maquinas de la empresa. La entrada al sistema por parte de un pirata informático no tendría muchas consecuencias al realizar un buffer overflow, solo quedaría como una violación al sistema de autenticación y autorización, pero durante un ataque de denegación de servicio los efectos siempre serian dañinos para las maquinas de la empresa, ocasionando en la reducción del servicio ofrecido por parte de la empresa hasta la perdida total del sistema.[9]

La principal solución para este problema es la prevención que debe de tener una empresa para un ataque DoS, es que no se debe de pensar que se es una empresa chica o poco importante para un ataque DoS los piratas informáticos

---

[7] *ibíd.*
[8] *Ibíd.*
[9] Areitio, Javier, Seguridad de la información redes, informática y: sistemas de información (Madrid: Paraninfo, 2008) pág. 164.

muchas veces no solo buscan dañar una empresa para obtener algo beneficios.

Figura 2 Ataque DoS (Denial of Service). Prevención para un ataque DoS (Creación propia)

La empresa debe tener un departamento de TI que esta constante mente prevenida para un ataque DoS. Se debe de estar siempre preparado para un ataque con sistemas de seguridad anti-DoS que puedan avisar de un inminente ataque, reduzca el trafico durante el ataque pero primordialmente que lo detenga. La utilización de cortafuegos es primordial para solucionar este tipo de problemas para poder eliminar este tipo de ataques, herramientas anti ataques DoS que evitaran la saturación de la red durante el ataque y mantener escaneada constantemente la red en tiempo real, ver su comportamiento para poder identificar cuando a se inicie esta amenaza. En conclusión las empresas deben tener departamentos de TI bien preparados para poder identificar y detener un ataque DoS, mantenerse constantemente actualizadas sus maquinas para evitar fallos en la seguridad. Tener siempre un plan desarrollado para saber como reaccionar y realizar un contrataque así de esta forma eliminar el problema.[10]

4. Tipos de Virus Informáticos

Los virus informáticos son un malware que tiene por objeto alterar el normal funcionamiento de una computadora sin el permiso o conocimiento del usuario. Estos virus se crean del mismo modo que cualquier programa. Son series de instrucciones que ordenan a las computadoras que hacer, contiene órdenes específicas para modificar los programas que contiene la computadora.[11]

[10] *Ibíd.*
[11] Orosco, Marta (et al), Informática 1 (México, Thompson, 2006) pág. 193

Estos pueden auto duplicarse y son archivos ocultos que se escriben sobre otros programas. Están diseñados para activarse al realizarse ciertas funciones o en determinada fecha y toman el control de la maquina afectada. A continuación conoceremos los distintos tipos de virus.[12]

Los Códigos Malicioso (o malware) hoy en día los conocemos como virus, si bien existen diferencias entre códigos maliciosos atendiendo el modo en que se instalan y se propagan. Los virus son un código malicioso que se incrusta dentro del código normal de un programa. Este virus se propaga de una computadora a otra y para ello se necesita de la intervención humana. Estos pueden tener un daño desde leve a muy grave sobre su objetivo. Aunque hoy en día es más frecuente que una computadora se infecte por medio de gusanos o troyanos. Además de estos virus existen también los gusanos este es un subtipo de virus, la principal diferencia es que el gusano no necesita de intervención humana para propagarse ya que lo hace automáticamente y no necesita alojarse en el código y se adueña de los servicios que se encarga de la transmisión de datos para tomar el control. Uno de los gusanos mas conocidos surgió en el 2003 llamado Blaster, este aprovecha la vulnerabilidad del servicio DCOM para mandar un mensaje al usuario del apagado inminente del equipo haciendo una cuenta atrás después de la cual el equipo se apagaba sin que fuera posible hacer nada por evitarlo. Otro virus de tipo gusano llamado Conficker fue conocido en 2008 que ataca el sistema operativo Windows hasta la versión de Windows 7 beta, se propaga a si mismo utilizando una vulnerabilidad del servicio Windows server. Otros nombres con el que se le conoce a este mismo virus son: Downup Devian, Downandup y kido. El troyano. Denominado caballo de Troya haciendo referencia ala mítica guerra de Troya. El troyano es un programa dañino con apariencia de software útil y absolutamente normal que puede resultar una importante amenaza para la seguridad informática. Un subtipo de troyano es el backdoor o puerta trasera este es un programa cliente-servidor que abre una puerta en el equipo cliente y que a través de esta el servidor toma posesión como si fuera propio lo que le permite tener acceso a todos los archivos, programas, contraseñas, correos electrónicos o descargados de internet, toda esta información los delincuentes informáticos la pueden utilizar para modificarla o utilizarla con fines ilícitos.[13] Un Bot malicioso también conocido como wwwbot o robot web. Bot es la simplificación de robot y se trata de cualquier programa, realizado en cualquier lenguaje de programación, que pretende emular al ser humano. Los Bot maliciosos son troyanos con funcionalidad de backdoor, una particularidad de este tipo de virus es que es que se instalan en las computadoras vulnerables por medio rastreo de internet. Una vez infectado el equipo el bot manda una señal a su creador y el equipo empieza a formar parte de un botnet, o red de

---

[1212] *Ibid.* Ver también Marroquín, Néstor, tras los pasos de un hacker (NMC Resarch Cia. Ltda, Ecuador 2010)

[13] Aguilera, Purificación, Seguridad Informática, (Editex, 2010) pág. 102

bots. A los bots también se les llama zombies por que cumplen las órdenes que reciben de los delincuentes cibernéticos.[14]

Spyware o programa espía. Es un código malicioso que para instalarse en una computadora necesita la participación de un virus o un troyano, aunque también podría estar oculto en los archivos de instalación de un programa normal. Este virus se dedica a extraer información de los usuarios y de su computadora. El objetivo mas leve y el mas común es aportar esos datos a las empresas que a partir de ese momento y por distintos medios principalmente por correo electrónico o pop-ups enviaran publicidad al usuario sobre los diferentes temas que le interesen. Debido a que este programa puede explorar con facilidad toda la información personal que el usuario tenga en su computadora como: listas de contactos información recibida (como pueden ser: números de tarjetas de crédito o de cuentas bancarias, domicilio, teléfonos etc.) software que este instalado en el equipo, direcciones IP, servidor de internet que utiliza, paginas web que visita constantemente, el tiempo que permanece en un sitio web como llevar a la quiebra a las empresa debido a la filtración de información confidencial.[15]

Virus de macro (macro instrucción) o también macro virus. Este es un subtipo de virus creado en modo macro, esta inscrito en un documento y no en un programa como los demás, si la computadora abre el documento infectado, la macro pasara a la biblioteca de macros de la aplicación que lo ejecute. Con lo que la macro lo ejecutara en sucesivos documentos que se abran con esa aplicación cuando se den las circunstancias en las que se haya programado.[16] En si podríamos decir que es muy variado los tipos de virus y muy peligrosos que incluso hasta pueden hacer que una empresa se valla a la quiebra. Por eso es de muchísima importancia estar actualizando constantemente los antivirus ya que estos detectan y eliminan la mayoría de los virus conocidos y tener nuestro equipo protegido y funcionando correctamente.

5. Intercepción de datos

La intercepción de datos por parte de terceras personas ajenas a la empresa que desean obtener información vital sobre las finanzas, estados de cuenta, contraseñas, etc. todo esto transmitido en la red de la empresa. Se debe de estar consiente de la situación de la red considerar que el 99.9% de los datos transmitidos no están cifrados y esto representa un gran problema en seguridad si alguien desea obtener la información transmitida ya que cualquiera podría interceptarlos. Esto no representaría un gran reto para un pirata

---

[14] *Ibíd.*

[15][15] *ibíd. Ver también Stallings, Williams, Fundamentos de seguridad en redes aplicaciones y estándares (Pearson Educación, Madrid 2004)*

[16] *Ibid,* pag. 103

informático. En internet se pueden encontrar una gran variedad de programas especialmente creados para inspeccionar una red, poder guardar la información transmitida en ella y luego poder inspeccionarla para poder encontrar la información mas importante como contraseñas introducidas, las paginas web consultadas, los documentos compartidos en la red, los e-mails enviados, información esencial sobre la empresa que el pirata informático desea obtener, estos programas se denominan “packet sniffer”.[17]

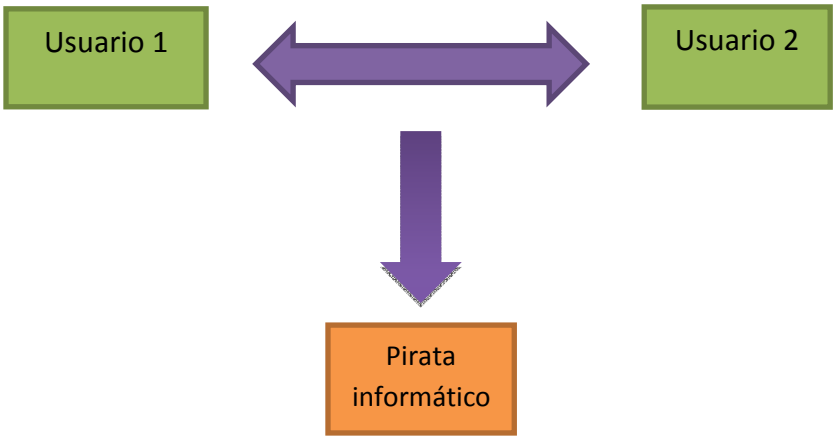

Figura 3 Intercepción de datos. Intercepción de datos por parte de un pirata informático (creación propia).

Dentro de una red todos los paquetes de datos que son enviados de una pc a otra son recibidos de forma sistemática por las maquinas. Cuando un ordenador ah recibido un paquete de datos inspecciona la dirección del ordenador que lo envió y realiza una comparación con su propia dirección. De esta manera únicamente el ordenador con la dirección de lo recibirá y podrá contestar.[18] Con este sistema de envió de datos por medio de la red se puede observar que un ordenador recibirá un paquete independientemente de que este no sea el destinatario. Considerando esto un pirata informático utilizaría un programa de espionaje para recibir estos datos, pudiendo guardarlos y leerlos para obtener la información deseada sin importa que estos paquetes de datos no estén destinados para su ordenador. [19]

En un tipo de red insegura dentro de una empresa los hubs simples no son seguros no son capaces de poder hacer un enrutamiento de acuerdo al paquete que se transmite. En el proceso de transmisión de datos en la red de la empresa en el momento en que un hub recibe un paquete de datos, se encarga de duplicarlo entonces lo manda a todos los puertos de salida, todas las maquinas conectadas a la red lo recibirán. De esta manera todas las

[17] Royer, Jean-Marc, Seguridad en la informática de empresa, (Barcelona, Ediciones ENI, 2004), pág. 22
[18] *Ibíd.*
[19] *Ibíd.*

maquinas recibirán este flujo de información de todas las maquinas, así el pirata informático podrá espiarlas a placer. De otra manera un conmutador de red, puede hacer la misma tarea que realiza un hub simple pero tiene mayor inteligencia. Cuando el conmutador de red recibe un paquete de datos sobre un puerto, solo lo enviara a la maquina de destino es aquí donde radica la inteligencia del conmutador a diferencia del hub que lo envía a todas, de esta manera se puede evitar que mande información a maquinas que no la requieren. De esta manera el conmutador mantendrá todas las maquinas conectadas a todos los puertos pero nunca recibirán los datos que tienen destinados, seria físicamente imposible que los recibieran dando mayor seguridad a la red de la empresa.[20]

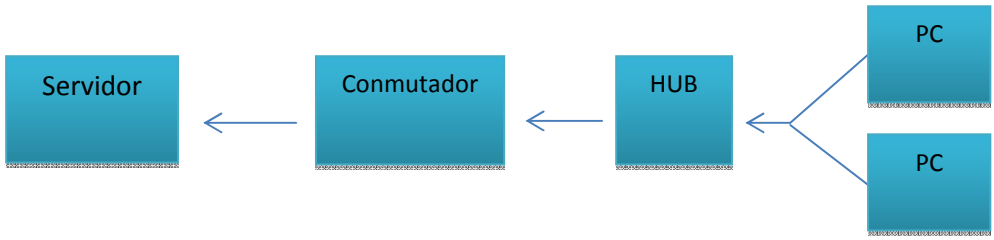

Figura 4 intercepción de datos. Red segura con conmutador (creación propia).

En conclusión la intercepción de datos en las empresas un problema muy serio no se debe pensar que se es una empresa pequeña como para no ser victima de un robo de información de este tipo. Se tienen registros de empresas que han tenido perdidas millonarias debido a este problema ya que muchas empresas no lo toman como un problema, pero esta ahí y se debe de estar preparado. Muchas empresas que brindan el servicio de internet hoy en día brindan un servicio especializado para las empresas con mayor seguridad. La utilización de conmutadores es clave para mantener un mayor control sobre la información que se transmite en la red de la empresa. Una gran solución para este problema es la encriptación de los datos de esta manera los datos estarán mas seguros.[21]

6. Solución a los principales problemas que amenazan la seguridad

Cada vez las empresas tienen a estar mas comunicadas entre si tanto con otras empresas como son sus clientes, esto ah motivado a una gran transmisión constante información es ahí donde se generan problemas de seguridad. Conforme la empresa crece se debe tener una mayor seguridad en ella, desde la creación de un departamento dedicado a la seguridad en las redes computacionales que mantendrá vigilada constantemente y mantener contralada la información que se maneja dentro de la empresa. Las empresas

[20] *Ibíd.*
[21] *Ibíd.*

deben de comer por tener una cultura de la seguridad dentro de ella, capacitar a sus empleados constante mente para tener un mayor control sobre la información que se maneja. En mayor problema de seguridad de las empresas son los empleados que muchas veces carecen de preparación para el manejo de información. Muchas veces los empleados generar grandes perdidas de información sin siquiera saberlo debido a la falta de cultura que existe en ellos, un ejemplo de esto es la utilización del internet de la empresa para fines personales como es la entrada sitios web que nada tienen que ver con la actividad que desempeñan. Muchas de las páginas web que existen en internet no son seguras o enlazan a sitios que pueden tener contenido malicioso como virus o spyware. Las medidas que debe de tomar la empresa con respecto a esto es el bloqueo de sitios web que no tengan que ver con la empresa. Otro problema ocasionado por los empleados es el mal manejo de correo electrónico, solo se debe de utilizar con fines que sean parte de la empresa, ocultar los contactos a la hora de enviar correos de esta manera no mostrar información que es vital para la empresa.[22]

Sobre el pirateo informático la empresa sobre la información que adquirirá, debe tener cuidado al adquirir software siempre debe tener una licencia, durante el uso de correo electrónico se debe de estar seguro sobre quien es el que ha mandado el correo ya que muchas veces hay correos electrónicos piratas que parecen ser de empresas como bancos que solo enlazan a paginas web pitaras cuyo objetivo es el robo de información como contraseñas, esto puede tener un alto costo para la empresa, al igual en el uso de las paginas web existen sitios que son piratas que tienen este mismo fin, los usuarios deben saber identificar cuales son las características que los diferencias de los originales. [23]

La red de la empresa es el punto cable en cuanto a seguridad se refiere la utilización de cortafuegos es primordial ya que previene de ataques maliciosos como lo son la denegación de servicio (DoS).[24]La solución ah esto tener en cuenta que siempre se puede ser victima de un ataque de este tipo y estar preparado para ello. Siempre tener monitoreada la red de la empresa para estar al tanto de como se comporta la transmisión de datos así poder identificar el problema y actuar rápido antes de que pueda ocurrir un paro total en el sistema. Con la implementación del cortafuegos se puede detener también el código malicioso, en conjunto con los antivirus, los cuales siempre deben de estar actualizados ya que existen muchos tipos de virus y spyware que pueden afectar gravemente al desempeño de las maquinas. Día con día surgen nuevas amenazas en el campo de los virus le departamento de informática deberá

[22] Areitio, Javier, Seguridad de la información redes, informática y: sistemas de información (Madrid: Paraninfo, 2008) pág. 3.
[23] Aceituno, Vicente, Seguridad de la Información, (Creaciones Copyright, 2004) pág. 12.
[24] Areitio, Javier, Seguridad de la información redes, informática y: sistemas de información (Madrid: Paraninfo, 2008) pág. 164. v

mantener constantemente escaneadas las maquinas para asegurar de que ningún virus pueda dañarlas. En conjunto con el spyware que ah diferencia de los virus este solo busca espiar la información que se maneja en las maquinas es así como también podrían obtener información de la empresa. Una forma muy común de contagiar una maquina en una empresa es por medio de memorias usb, muchas veces los empleados llevan trabajo a casa, las utilizan en una maquina que esta infectada y al momento de conectarla en la maquina de la empresa es cuando surge la infección.[25] La empresa debe tener un control sobre esto mediante los antivirus y antispyware, capacitar a los empleados en todas estas medidas de seguridad que parecen muy simples pero que pueden tener un gran costo para la empresa, un paro en el servicio puede significar una perdida importante en ganancias tanto para la empresas como para sus clientes.

[25] Aguilera, Purificación, Seguridad Informática, (Editex, 2010) pág. 102

Bibliografía

Monografía

Aceituno, Vicente, Seguridad de la Información, (Creaciones Copyright, 2004)
Aguilera, Purificación, Seguridad informática, (Editex, 2010)
Areito, Javier, Seguridad de la información redes, informática y: sistemas de información (Madrid, Paraninfo, 2008)
Orosco, Marta (et al), Informática 1 (México, Thompson, 2006)
Royer, Jean-Marc, Seguridad en la informática de empresa, (Barcelona, Ediciones ENI, 2004).