NIVELES DE SEGURIDAD LÓGICA CONTRA ATAQUES EXTERNOS A TRAVÉS DE INTERNET EN UNA PLATAFORMA WINDOWS 2000 SERVER EN EMPRESAS DE TECNOLOGÍA

LOGICAL SECURITY LEVEL VS EXTERNAL ATTACKS FROM INTERNET IN A WINDOWS 2000 SERVER PLATFORM IN TECHNOLOGICAL COMPANIES

Lisbeth Mora
Universidad Rafael Belloso Chacín. Venezuela.

RESUMEN

La introducción de Internet en el mundo de los negocios aumenta a pasos agigantados, las acciones para mantener la seguridad de los sistemas conectados a Internet es una preocupación fundamental por las pérdidas económicas en términos de información robada o perdida. El objetivo de este trabajo es analizar los niveles de seguridad lógica contra ataques externos a través de Internet en una plataforma Windows 2000 Server, en las empresas de tecnología de información, para lo cual fue necesario identificar los tipos de ataques y los métodos de mitigación. El tipo de investigación fue aplicado, descriptivo y su diseño fue no experimental transeccional. La población estuvo conformada por 60 empresas y la muestra se seleccionó con el criterio de muestra de expertos en el área de redes de información. La técnica utilizada para la recolección de datos fue la entrevista y el instrumento fue el cuestionario, el mismo estuvo conformado por 42 preguntas, realizadas a fin de determinar el conocimiento de los ataques realizados por Internet, sus frecuencias, consecuencias, mecanismos y configuraciones implementados para mitigarlos. Los resultados de los cuestionarios fueron expresados según los cálculos de frecuencia relativa y acumulada asociados a los daños ocasionados y formas de detección utilizadas. Como resultado de la investigación se detectó que los intrusos informáticos utilizan su ingenio para acceder a sistemas operativos sin autorización, esto conlleva a la dificultad de detectarlos por parte de los administradores de redes. Aunado a esto la falta de medidas de protección que mantienen las empresas ponen en alto riesgo su servicio de redes, por lo cual se propuso la creación de políticas de seguridad basadas en los lineamientos referidos por Microsoft que permiten minimizar los riesgos y evitar los ataques que existen en Internet.

Palabras claves: Política de Seguridad, Riegos, ataques, Amenaza, Intrusos informáticos.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 4 Edición No 2 – Año 2005

ABSTRACT

The introduction of Internet in the world's businesses increases to exaggerated steps, the actions to maintain the security of the connected systems to Internet is a fundamental preoccupation by the economic losses in terms of robbed or lost information. The objective of this work is to analyze the levels of Logical Security against external attacks through Internet in a Windows 2000 Server in the companies of Information Technology, it was necessary to identify the types of attacks and the methods of mitigation. The type of investigation is applied, descriptive and its design was nonexperimental transaccional. The population was formed by 60 companies and the sample was selected with the criterion of 9 experts in the area of networks. The technique used for the data collection was the interview, and the instrument was the questionnaire conformed by 42 questions, to find the knowledge of the Internet's attacks, its frequencies, consequences, and the mechanisms and implemented configurations to mitigate them. The results of questionnaires were expressed according to the calculations of frequency relative and accumulated, associated to damages and used forms of detection. As result of this investigation, is detected that informatics intruder uses their abilities to access into operating system without an authorization, then, it become a trouble due that they cannot be found by network administrators. In addition to the lack of protection measures that put in high risk the service of the organization's networks, thus it is recommended the creation of policies of security based on the politics referred by Microsoft that allow to minimize the risks and reduce the attacks on Internet.

Key Words: Policy of Security, Irrigations, attacks, Threat, Intruders.

INTRODUCCIÓN

En los últimos años el desarrollo tecnológico impulsado por los procesos de innovación ha crecido de manera considerable, particularmente en Venezuela con la apertura a las telecomunicaciones y el apoyo del estado, para la implantación de nuevas tecnologías como Internet y la convergencia de voz, datos y video, ha sumergido a las empresas en una nueva sociedad tecnológica.

Son indudable los beneficios que estas innovaciones traen para las organizaciones a nivel de competitividad y rentabilidad, no obstante se han convertido en un elemento de riesgo, por cuanto que se reportan en las redes de información, situaciones de acceso no autorizado, modificación o eliminación de archivos confidenciales, caída inesperada e inexplicable de los servicios de red y de los servidores.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 4 Edición No 2 – Año 2005

En la mayoría de los casos estas fallas de seguridad son ocasionadas por personas inescrupulosas que hacen uso de sus habilidades y conocimientos técnicos para infiltrarse a través de las redes telemáticas, estas personas son identificas a nivel mundial con denominaciones como Hackers y Crackers. Cabe destacar que gran parte de estas intromisiones son efectuadas por personal interno de confianza, que de manera no intencional en algunos casos, provocan estas fallas de seguridad.

Por otra parte, las mismas tecnologías de la información y comunicaciones, por la rapidez con que son introducidas al mercado o la complejidad de sus configuraciones, presentan ciertas vulnerabilidades que ofrecen una puerta de acceso a los intrusos.

Ante esta situación se hace necesario analizar los niveles de seguridad implementados en empresas de tecnología para apoyar el diseño y organización de mecanismos de seguridad que ayuden a mitigar los riesgos y las vulnerabilidades tecnológicas.

Por lo tanto, esta investigación busca analizar los niveles de seguridad lógica que presentan las empresas de tecnología a fin de plantear un modelo adaptado a las necesidades usadas en Venezuela, que se convierta en una herramienta de consulta para los gerentes y responsables de los servicios tecnológicos, a fin de identificar cuales son los principales ataques y vulnerabilidades; y cuales son las recomendaciones para su mitigación e implantación.

OBJETIVOS DE LA INVESTIGACIÓN

El propósito de esta investigación es analizar los niveles de seguridad lógica contra ataques externos a través de Internet en una plataforma Windows 2000 Server, en las empresas de Tecnología de Información.

Para poder cumplir con este objetivo se llevaron a cabo las siguientes actividades: (a) identificar los ataques realizados por personas desautorizadas que afecten la seguridad lógica de la plataforma Windows 2000 Server en las empresas de tecnología. (b) identificar los ataques realizados por programas que acceden a través de Internet al Sistema Windows 2000 Server en las empresas de tecnología. (c) determinar los mecanismos de mitigación que permiten la protección ante los ataques realizados por usuario y por programas, a través de Internet en la plataforma Windows 2000 Server de las empresas de tecnología.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 4 Edición No 2 – Año 2005

METODOLOGÍA

De acuerdo a las diferentes clasificaciones existentes sobre tipos de estudios en esta investigación se utilizó el descriptivo, documental, dado a que se exponen las manifestaciones de ataques externos y las consecuencias de su acceso en la información de las empresas de tecnologías.

El tipo de diseño fue no experimental, dado a que las variables no estuvieron sujetas a modificaciones intencionales por parte del investigador. (Hernández, Fernández, y Batista, 1997). A su vez, esta investigación pertenece al tipo transaccional, tomando en cuenta que la descripción de los sucesos evaluados se realizó una sola vez y en tiempo determinado. Hernández et. al. (2003) indica que estos tipos de diseños de investigación recolectan datos en un único momento, su propósito es describir variables y analizar su incidencia en un momento dado.

ANTECEDENTES DE LA INVESTIGACIÓN

Las siguientes tesis relacionadas con la seguridad de la información fueron revisadas, con el fin de tomar los aspectos más resaltantes que contribuyeron a la realización de esta investigación:

Tal es el caso el Trabajo de Grado presentado por Prada Jorge, en el año 2000, titulado: Diseño de redes de seguridad de datos de una empresa de servicios de tecnología de investigación presentada en la Universidad Rafael Belloso Chacín. Esta investigación se realizó con el objeto de proponer un diseño de redes de seguridad de datos en una empresa de servicios de tecnología de información. El diagnóstico de la investigación dio como resultado la falta de medidas de protección que pone en alto riesgo el servicio de redes de la organización, por lo cual se propuso un diseño mediante el uso de un modelo de seguridad integral que permita mitigar los riesgos y reducir las amenazas existentes de una manera costo efectiva.

El siguiente estudio considerado fue desarrollado por Luís Ugas, titulado: Seguridad en organizaciones con tecnologías de información. El propósito del trabajo fue el de identificar los factores organizacionales que incidían en la seguridad, evaluar los niveles de importancia y de riesgo de cada uno de esos factores y presentar el diseño de una propuesta de solución. Esta investigación concluyó que la mayoría de las organizaciones de tecnología de información no existen los niveles adecuados de seguridad que garanticen la confiabilidad, la integridad y la disponibilidad de la información, y que las personas que las integran no poseen una cultura organizacional de

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 4 Edición No 2 – Año 2005

seguridad. Razón por la cual, se diseñó un modelo de seguridad dinámico que sirviera de marco referencial para la implantación y mantenimiento de un esquema de seguridad.

Otro aporte fue la Tesis Doctoral de Ugas Luís, titulada: Uso y difusión de las tecnologías de Internet para el acceso a la sociedad red. El objetivo propuesto fue determinar el nivel de uso y difusión de las tecnologías de Internet para el acceso a la sociedad red, por parte de los ciudadanos del Municipio Maracaibo del Estado Zulia. De acuerdo a los detalles en esa investigación referidos a los bajos niveles de uso por el nivel de alfabetismo tecnológico y la brecha digital existente se recomendó impulsar la universalización del acceso a Internet, incentivar el desarrollo de contenidos nacionales en Internet, fomentar el desarrollo de las habilidades informativas y establecer un sistema de indicadores de las TIC para Venezuela.

CONSIDERACIONES TEÓRICAS

Las bases teóricas utilizadas como soporte conceptual para la presente investigación abordan aspectos generales relacionados con la seguridad de la información, tipos de riesgos y amenazas y mecanismos de mitigación.

CONCEPTOS DE SEGURIDAD

En la actualidad, la seguridad informática ha adquirido gran auge, dadas las cambiantes condiciones y las nuevas plataformas de computación disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes que permiten explorar más allá de las fronteras de la organización.

POLÍTICAS DE SEGURIDAD INFORMÁTICA (PSI)

Una política de seguridad informática es una forma de comunicarse con los usuarios y los gerentes. Las PSI establecen el canal formal de actuación del personal, en relación con los recursos y servicios informáticos, importantes de la organización. (Chapman y Zwicky, 1997).

No se trata de una descripción técnica de mecanismos de seguridad, ni de una expresión legal que involucre sanciones a conductas de los empleados. Es más bien una descripción de los que deseamos proteger y el por qué de ello.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 4 Edición No 2 – Año 2005

NIVELES DE TRABAJO PARA ESTABLECER PSI

Para Bello (1998), los niveles de trabajo lo conforman los siguientes servicios que permiten levantar los procedimientos de las políticas de seguridad:

a) Confidencialidad: consiste en proteger la información contra la lectura no autorizada explícitamente.

b) Integridad: es necesario proteger la información contra la modificación sin el permiso del dueño.

c) Autenticidad: en cuanto a telecomunicaciones se refiere, la autenticidad garantiza que quien dice ser "X" es realmente "X".

d) No repudio: ni el origen ni el destino en un mensaje deben poder negar la transmisión.

e) Disponibilidad de los recursos y de la información: de nada sirve la información si se encuentra intacta en el sistema pero los usuarios no pueden acceder a ella.

f) Consistencia: se trata de asegurar que el sistema siempre se comporte de la forma esperada, de tal manera que los usuarios no encuentren variantes inesperadas.

g) Control de acceso a los recursos: consiste en controlar quién utiliza el sistema o cualquiera de los recursos que ofrece y cómo lo hace.

h) Auditoria: consiste en contar con los mecanismos para poder determinar qué es lo que sucede en el sistema, qué es lo que hace cada uno de los usuarios y los tiempos y fechas de dichas acciones.

AMENAZAS A LA SEGURIDAD DE LA INFORMACIÓN

Se entiende por amenaza a la seguridad de la información, una condición del entorno del sistema de información que dada una oportunidad, podría producir una violación de la seguridad (confidencialidad, integridad, disponibilidad).

Según Marcano (2003), las amenazas a la seguridad en una red pueden caracterizarse modelando el sistema como un flujo de información que viene

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 4 Edición No 2 – Año 2005

desde una fuente, como por ejemplo un archivo ubicado en la memoria principal, a un destino, que puede ser otro archivo o un usuario.

González (2003), selecciona las amenazas en las siguientes categorías:

a) Interrupción**:** un recurso del sistema es destruido o se vuelve no disponible, este ataque es contra la disponibilidad. Ejemplos: destrucción de un disco duro.

b) Intercepción: una entidad no autorizada consigue acceso a un recurso, éste es contra la confidencialidad.

c) Modificación**:** una entidad no autorizada no sólo consigue acceder a un recurso, sino que es capaz de manipularlo.

d) Fabricación*:* una entidad no autorizada inserta objetos falsificados en el sistema.

ADMINISTRACIÓN DE RIESGOS

No existe un entorno de informático totalmente seguro y al mismo tiempo útil. Al examinar el entorno, se deberá evaluar los riesgos que sufre actualmente, determinar un nivel de riesgo aceptable y mantener el riesgo a ese nivel o por debajo del mismo. Según, Borghello (2003), estos incluyen recursos, amenazas, vulnerabilidades, explotaciones y contramedidas.

1. Recursos: es cualquier elemento del entorno que intente proteger. Puede tratarse de datos, aplicaciones, servidores, enrutadores e incluso personas.

2. Amenazas: es una persona, un lugar o un elemento que puede tener acceso a los recursos y dañarlos.

3. Vulnerabilidades: es un punto en el que un recurso es susceptible de ser atacado. Se puede interpretar como un punto débil.

4. Explotación: una amenaza que se aprovecha de una vulnerabilidad del entorno puede tener acceso a un recurso. Este tipo de ataque se denomina explotación.

5. Contramedidas: se aplican para contrarrestar las amenazas y vulnerabilidades y de este modo reducir el riesgo en el entorno.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 4 Edición No 2 – Año 2005

CONTROL DE ACCESO EXTERNO

Los controles de acceso pueden implementarse en el sistema operativo, sobre los de aplicación, en bases de datos, en un paquete específico de seguridad o en cualquier otro utilitario.

Para Borgello (2001) los controles de acceso constituyen una importante ayuda para proteger al sistema operativo de la red, al sistema de aplicación y demás software de la utilización o modificaciones no autorizadas; para mantener la integridad de la información y para resguardar la información confidencial de accesos no autorizados. Entre los tipos de accesos se encuentran:

1. Dispositivos de control de puertos: autorizan el acceso a un puerto determinado y pueden estar físicamente separados o incluidos en otro dispositivo de comunicaciones, como por ejemplo un módem.

2. Firewalls o puertas de seguridad: permiten bloquear o filtrar el acceso entre dos redes, usualmente una privada y otra externa (por ejemplo Internet).

3. Acceso de personal contratado o consultores: debido a que este tipo de personal en general presta servicios temporarios, debe ponerse especial consideración en la política y administración de sus perfiles de acceso.

4. Accesos públicos: para los sistemas de información consultados por el público en general, o los utilizados para distribuir o recibir información computarizada.

Por otro lado para llevar mayor control de seguridad es importante mantener normas y procesos basados en técnicas aprobadas por grandes empresas de tecnología, tal es caso del próximo punto a tratar.

MICROSOFT OPERATIONS FRAMEWORK (MOF)

Para que las operaciones del entorno funcionen de la forma más eficaz, se deben administrar de forma efectiva. Microsoft desarrolló Microsoft Operations Framework (MOF). Sus instrucciones permiten garantizar la seguridad, la confiabilidad, la disponibilidad, el soporte y la capacidad de administración de sus sistemas de producción fundamentales.

El modelo de procesos MOF se divide en cuatro cuadrantes integrados de la manera siguiente: (1) Cambio, (2) Funcionamiento, (3) Soporte, (4)

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 4 Edición No 2 – Año 2005

Optimización. Juntas, las fases forman un ciclo de vida en espiral que se puede aplicar a todo, desde una aplicación específica a un entorno de operaciones completo con varios centros de datos.

SERVICIOS DE SEGURIDAD PARA WINDOW 2000 SERVER

Microsoft lanzó una iniciativa en octubre de 2001, denominada Programa estratégico de protección de tecnología (STPP, Strategic Technology Protection Program). El objetivo de este programa es integrar los productos, los servicios y el soporte de Microsoft dedicados a la seguridad.

Microsoft divide el proceso de mantener un entorno seguro en dos fases relacionadas: a) Implementar la seguridad: constituye la primera fase del STTP, basado en seguir las recomendaciones, especificadas en el Microsoft Security Tool Kit, donde recursos, parches y services packs que darán alta protección a los servidores conectados a Internet. b) Mantener Seguridad: constituye la segunda fase del STTP se refiere a la adopción medidas preventivas contra las amenazas y responder con eficacia cuando se produzcan.

DEFENSA EN PROFUNDIDAD

Para lograr esta defensa, Microsoft (2004) creó la estrategia defensa en profundidad, denominada también seguridad en multicapa, procede de un término militar utilizado para describir la aplicación de contramedidas de seguridad con el fin de formar un entorno de seguridad cohesivo sin un sólo punto de error.

DEFENSA DE DATOS

A nivel de cliente, los datos almacenados localmente son especialmente vulnerables. Si se roba un equipo portátil, es posible realizar copias de seguridad, restaurar y leer los datos en otro equipo, aunque el delincuente no pueda conectarse al sistema.

DEFENSA DE APLICACIONES

Como una capa de defensa más, el refuerzo de las aplicaciones es una parte esencial de cualquier modelo de seguridad. Muchas aplicaciones utilizan el subsistema de seguridad de Windows 2000 para proporcionar seguridad.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 4 Edición No 2 – Año 2005

DEFENSA DE HOSTS

El refuerzo de la defensa de los Hosts constituye otra capa de protección importante, por lo que se debe evaluar cada host del entorno y crear directivas que limiten cada servidor sólo a las tareas que tenga que realizar.

DEFENSA DE REDES

Si se dispone de una serie de redes en la organización, éstas deben ser evaluadas individualmente para asegurarse de que se ha establecido una seguridad apropiada.

DEFENSA DE PERÍMETROS

La protección del perímetro de la red es el aspecto más importante para detener los ataques externos. Si el perímetro permanece seguro, la red interna estará protegida de ataques externos.

AMENAZAS LÓGICAS

La identificación de amenazas requiere conocer los tipos de ataques, el tipo de acceso, la forma operacional y los objetivos del atacante. Las consecuencias de los ataques se podrían clasificar en:

a) Data Corruption: la información que no contenía defectos pasa a tenerlos.

b) Denial of Service (DoS): servicios que deberían estar disponibles no lo están.

c) Leakage: los datos llegan a destinos a los que no deberían llegar.

Howard (1995) indica en su estudio, la cantidad de ataques que puede tener un incidente. Al concluir dicho estudio y basado en su experiencia en los laboratorios del CERT afirma que esta cantidad varía entre 10 y 1.000 y estima que un número razonable para estudios es de 100 ataques por incidentes.

TIPOS DE ATAQUE

A continuación se expondrán diferentes tipos de ataques perpetrados, principalmente, por Hackers. Estos ataques pueden ser realizados sobre cualquier tipo de red, sistema operativo, usando diferentes protocolos, etc.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 4 Edición No 2 – Año 2005

ATAQUES DE MONITORIZACIÓN

Este tipo de ataque se realiza para observar a la víctima y su sistema, con el objetivo de obtener información, establecer sus vulnerabilidades y posibles formas de acceso futuro.

ATAQUES DE AUTENTIFICACIÓN

Este tipo de ataque tiene como objetivo engañar al sistema de la víctima para ingresar al mismo; generalmente se realiza tomando las sesiones ya establecidas por la persona u obteniendo su nombre de usuario y password.

DENEGACIÓN DE SERVICIO (DOS)

Los protocolos existentes actualmente fueron diseñados para ser empleados en una comunidad abierta y con una relación de confianza mutua. La realidad indica que es más fácil desorganizar el funcionamiento de un sistema que acceder al mismo; así los ataques de negación de servicio tienen como objetivo saturar los recursos de la víctima de forma tal que se inhabilita los servicios brindados por la misma.

ATAQUES DE MODIFICACIÓN – DAÑO

Este ataque es la modificación sin autorización de los datos o el software instalado en el sistema víctima, incluyendo borrado de archivos. Son particularmente serios cuando el que lo realiza ha obtenido derechos de administrador o supervisor, con la capacidad de disparar cualquier comando y por ende alterar o borrar cualquier información que puede incluso terminar en la baja total del sistema.

VIRUS INFORMÁTICO (VI)

Se define como pequeño programa, invisible para el usuario (no detectable por el sistema operativo) y de actuar específico y subrepticio, cuyo código incluye información suficiente y necesaria para que, utilizando los mecanismos de ejecución que le ofrecen otros programas a través del microprocesador, puedan reproducirse formando réplicas de sí mismos susceptibles de mutar; resultando de dicho proceso la modificación, alteración y/o destrucción de los programas, información y/o hardware afectados (Virus Report (2000).

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 4 Edición No 2 – Año 2005

REPRODUCTORES – GUSANOS

Son programas que se reproducen constantemente hasta agotar totalmente los recursos del sistema huésped y/o recopilar información relevante para enviarla a un equipo al cual su creador tiene acceso.

CABALLOS DE TROYA

De la misma forma que el antiguo caballo de Troya de la mitología griega, escondía en su interior algo que los troyanos desconocía, y que tenía una función muy diferente a la que ellos podían imaginar; un caballo de Troya es un programa que aparentemente realiza una función útil pero además realiza una operación que el usuario desconoce y que generalmente beneficia al autor del troyano o daña el sistema huésped.

PROGRAMA ANTIVIRUS

Un antivirus constituye una gran base de datos con la huella digital de todos los virus conocidos para identificarlos y también con las pautas que más contienen los virus. Según Borgello (2001), los fabricantes de antivirus avanzan tecnológicamente casi en la misma medida que lo hacen los creadores de virus.

FIREWALL

Un Firewall es un sistema (o conjunto de ellos) ubicado entre dos redes y que ejerce la una política de seguridad establecida. Es el mecanismo encargado de proteger una red confiable de una que no lo es (por ejemplo Internet) Borgello (2001). Puede consistir en distintos dispositivos, tendientes a los siguientes objetivos: a) Todo el tráfico desde dentro hacia fuera, y viceversa, debe pasar a través de él, b) Sólo el tráfico autorizado, definido por la política local de seguridad, es permitido.

ROUTERS Y BRIDGES

Cuando los paquetes de información viajan entre su destino y origen, vía TCP/IP, pasan por diferentes Routers (enrutadores a nivel de red). Los Routers son dispositivos electrónicos encargados de establecer comunicaciones externas y de convertir los protocolos utilizados en las LAN en protocolos de WAN y viceversa. En cambio, si se conectan dos redes del tipo LAN se utilizan Bridges, los cuales son puentes que operan a nivel de enlace

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 4 Edición No 2 – Año 2005

CONCLUSIONES

Las siguientes conclusiones se realizaron en función de los criterios asociados al objetivo general y los objetivos específicos desarrollados en esta investigación. En relación a los ataques realizados por intrusos informáticos se concluye que: los responsables de las redes de empresas de tecnologías reconocen los Hacker y Crackers. Estos personajes representan una grave amenaza a la información debido a que utilizan sus habilidades en programación para alterar, destruir y apropiarse de la información de las empresas.

El promedio mensual de ataques recibidos es elevado, ocasionando en la mayoría casos daños leves. La mayoría de los administradores de la red no logran reconocer los ataques proporcionados por intrusos informáticos debido a lo difícil que resulta rastrear sus huellas, resultando el diagnóstico de un antivirus o software experto la principal forma de detección de virus y de ataques, a pesar de esto la mayoría de los ataques se detecta cuando ya se ha causado un daño.

Un Cracker destruye información y puede causarle a la empresa daños millonarios alterando, destruyendo y sustrayendo datos, utilizando las técnicas de intercepción, modificación, fabricación. El número de detecciones de ataques causados por empleados descontentos en empresas, es menor que los ocasionados por Hackers y Cracker.

Con relación a los ataques realizados por programas se establecieron las siguientes conclusiones: los virus y los gusanos representan los principales tipos ataques señalados por los administradores de redes. El promedio de ataques por virus fue mayor que el realizado por los gusanos; ocasionando daños de todo tipo, sin embargo la mayor parte de ellos ocasionaron daños leves y moderados. Los ataques menos identificados fueron los realizados por caballos de Troya, sin embargo la consecuencia de daños fueron de tipo mayor.

En relación a los métodos de mitigación utilizados por los expertos se concluye que: los antivirus representan la principal forma de protección usada por los administradores de redes para resguardar los servidores Windows 2000 y estaciones de trabajo. Los antivirus y firewall utilizan diferentes algoritmos de scaneo, dicha tecnología disminuye el rendimiento del servidor. La avanzada tecnología de los antivirus y firewall los hace aplicaciones complicadas a la hora de ser manejadas por los responsables de la red.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 4 Edición No 2 – Año 2005

Los administradores de redes identifican la importancia de mantener normas y procedimientos para la correcta operatividad de sus antivirus y firewall, para garantizar la protección de los datos de la empresa. Sin embargo estas normas no incluyen aspectos importantes como la documentación de los pasos sobre instalación y configuración del servidor en casos desastres y la distribución organizada de los funciones de los responsabilidades.

En cuanto a las normativas de seguridad que mantienen las empresas se concluyó que la mayoría de los administradores de redes, implementan políticas de seguridad para minimizar el número de infecciones por virus, gusanos y por ataques de intrusos informáticos y empresariales. Sin embargo, no implementan medidas de seguridad físicas para proteger los sistemas y equipos en las empresas al no mantener políticas en el uso de contraseñas, la verificación de portátiles externos ingresados a la empresa y la verificación de archivos de entrada a la red, además de no contribuir con la difusión y enseñanza en materia de seguridad a los usuarios de la red.

RECOMENDACIONES

Las siguientes sugerencias surgen de las necesidades observadas en el proceso de análisis de resultados de esta investigación, están dirigidas a los administradores responsables de la información de empresas de tecnología. Las recomendaciones propuestas consisten en crear políticas de seguridad de información basadas en:

Mantener vigentes los conocimientos sobre nuevos riesgos y amenazas que afectan la información de la empresa, a través de talleres de capacitación. Los mismos deben incluir las últimas vulnerabilidades encontradas en los sistemas operativos y diferentes las aplicaciones Microsoft.

Mantener actualizada las versiones de los antivirus así como las definiciones de los virus. Instalar los Service Packs necesarios a las aplicaciones y sistemas señalados por la Corporación Microsoft.

Suscribirse en un plan de entrenamiento ofrecido por Microsoft y estar atentos a las nuevas vulnerabilidades en sistemas y aplicaciones encontradas por grandes empresas de tecnología tales como CERT, dedicadas a realizar investigaciones de alto nivel sobre amenazas en Internet.

Mantener respaldos de información periódicos y actualizados de

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 4 Edición No 2 – Año 2005

diferentes tipos, para minimizar el impacto de la empresa al enfrentar desastres informáticos.

Preparar y realizar talleres de capacitación sobre las amenazas y riesgos utilizando lenguaje sencillo a los trabajadores de empresas, a fin de minimizar puntos débiles en las redes.

Implementar políticas basadas en la evaluación del personal para brindar acceso restringido y seguro. Igualmente realizar ese tipo de acciones para conceder los accesos a Internet.

Se recomienda a las empresas de tecnología, contratar servicios especializados que garanticen el uso de aplicaciones y herramientas adecuadas, estadísticas de intentos frustrados y realizados y soluciones que abarquen las 24 horas de día.

Se recomienda a los centros de formación profesional en el área de computación, la integración en las cátedras de estudio materias relacionadas con la seguridad de información. Dichas materias deben indicar el funcionamiento de aplicaciones de antivirus, firewall y demás software expertos; de esta manera se formarán profesionales integrales que lleguen a las áreas de trabajo con una visión global sobre seguridad.

REFERENCIAS BIBLIOGRÁFICAS

Álvarez, M. (1997-2000). *Criptomicón, Seguridad Informática, Instituto de Física Aplicada del CSIC.* Recuperado el 17 de marzo de 2003, en http://www.prevencion-seguridadba.com/seguridad_informatica.

Bello, C. (1998) *Manual de Seguridad en Redes,* Recuperado el 20 de febrero de 2004 en http://www.seguridad.unam.mx/SemAU/Admin-UNAM-2002/Admin-UNAM-octubre/Auditoria.doc

Borghello, C. *Seguridad Informática. Sus implicaciones e implementaciones*. Recuperado el 17 de marzo de 2003, en http://www.webmaster@cfbsoft.com

Hernández, R.; Fernández, C. y Baptista, P. (1991). *Metodología de la Investigación. México,* México: Editorial McGraw-Hill.

Howard, J. *(*1989-1995). Tesis: *An Analysis of security on the Internet*. Carnegie Institute of Technology. Carnegie Mellon University. 1995. EE.UU. http://www.cert.org

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 4 Edición No 2 – Año 2005

Microsoft Corporation (2000). Guía para la implantación de Windows 2000 Server, Recopilado el 21de abril de 2004 en http://www.microsoft.com/spain/ technet/seguridad/programastpp.asp

Prada, J. (2000). *Diseño de Redes de Seguridad de datos de una empresa de servicios de tecnología de información*. Trabajo de Grado, Universidad Rafael Belloso Chacín, Decanato de Investigación y Postgrado, Maestría en Gerencia de Proyectos Industriales, Maracaibo, Venezuela.

Paz M. y Bara E. *Hackers, los piratas de la red, Archivo de prensa, Universidad Virtual 2003*. Recopilado el 21de marzo de 2003 en www.uvirtual.cl/prensa/reportajes

Saulo V. (2002). No solo de Tecnología vive el hombre, *Microsoft Revista: BSKnow* Recopilado el 21de marzo de 2003 en http://www.bs.com.ar/bsweb/RevistaBSknow/Revistajunio03PDF/Framework.pdf

Ugas, *L. (2001).* Seguridad en Organizaciones con Tecnologías e Información. Trabajo de Grado, Universidad Rafael Belloso Chacín, Decanato de Investigación y Postgrado, Maestría en Telemática, Maracaibo, Venezuela.

Ugas, L. (2003). *Uso y Difusión de las Tecnologías de Internet para el acceso a la Sociedad Red.* Tesis doctoral, Doctorado en Ciencias Gerenciales. Universidad Rafael Belloso Chacín, Vicerrectorado Investigación Gerenciales, Maracaibo, Venezuela.

Vidal R. (enero 2004, 27). Los ataques informáticos se multiplican, Belt Ibérica S.A. Analistas de Prevención. *Portal de profesionales en seguridad,* http://www.belt.es/noticias/2004/enero/12/ataques.htm

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 4 Edición No 2 – Año 2005