ISSN 0798 1015

REVISTA ESPACIOS

HOME | Revista ESPACIOS | ÍNDICES / Index | A LOS AUTORES / To the AUTHORS

Vol. 39 (Nº 42) Año 2018 • Pág. 19

Defensa en profundidad aplicado a un entorno empresarial

Depth defense applied to a business environment

Alfonso A. GUIJARRO-Rodríguez 1; Jessica M. YEPEZ-Holgin 2; Tania J. PERALTA-Guaraca 3; Mirella C. ORTIZ Zambrano 4

Recibido: 23/04/2018 • Aprobado: 08/06/2018

Contenido

RESUMEN:
El crecimiento exponencial que presentan las Tecnología de la Información y Comunicación (TIC´s) y la demanda del uso del internet como principal medio de transporte para las empresas, ha provocado que atacantes informáticos busquen vulnerabilidades en las infraestructuras de redes, atraídos por vencer la complejidad de la seguridad. Por ello, esta propuesta pretende, fortalecer los esquemas de red, mediante el uso de la metodología defensa en profundidad, para que los profesionales de IT que inician la protección de los datos cuenten con un esquema que reduzca significativamente los niveles de vulnerabilidades en las empresas. La metodología de este trabajo plantea un escenario de red empresarial compuesto por tres segmentos de red: LAN – WAN - DMZ. Luego de montar el esquema de red, se establecieron las gestiones necesarias en cada fase de la metodología defensa en profundidad y con ello se logró mitigar en forma precisa las constantes amenazas de seguridad que sufre una empresa, siendo esta propuesta una guía que reduce las vulnerabilidades no se convierte en una solución absoluta, puesto que la seguridad depende de la pericia del responsable a cargo y de cómo establece su diseño de red.
Palabras-Clave: Defensa en profundidad, seguridad informática, controlador de dominio, red empresarial.

ABSTRACT:
The exponential growth of Information and Communication Technology (ICTs) and the demand for the use of the internet as the main means of transportation for companies has caused computer attackers to look for vulnerabilities in network infrastructures, attracted by overcoming the complexity of security. Therefore, this proposal aims to strengthen network schemes, through the use of the defense in depth methodology, so that IT professionals who initiate data protection have a scheme that significantly reduces the levels of vulnerabilities in the Business. The methodology of this work proposes a business network scenario consisting of three network segments: LAN - WAN - DMZ. After assembling the network diagrams, the necessary steps were established in each phase of the defense-in-depth methodology and with this, it was possible to mitigate accurately the constant security threats that a company suffers, this proposal being a guide that reduces vulnerabilities it does not become an absolute solution, since security depends on the expertise of the person in charge and how it establishes its network design.
Keywords: Defense in depth, computer security, domain controller, business network

1. Introducción

El creciente uso de las Tecnologías de la Información y Comunicación (TIC´s) se debe a la demanda que existe por el Internet, hay personas que navegan en redes sociales, buscan información, realizan transacciones comerciales en sistemas informáticos entre otros. (Muñoz & Rivas, 2015), trabajos recientes, revelan el crecimiento exponencial que sufren los sistemas informáticos ante los diversos ataques de seguridad informática.

Los ataques que sufren las empresas tanto públicas como privadas, representan millones de dólares en pérdidas a nivel mundial cada año, razón por la cual, se deben desarrollar medidas preventivas que eviten posibles ataques y fallos de seguridad (Muñoz & Rivas, 2015).

Consientes que la seguridad informática, no se desarrolla a la par como los métodos para vulnerar sistemas, esta intentan disminuir el grado de vulnerabilidad que presentan los sistemas informáticos aplicando seguridad en capas, como es el caso de la metodología defensa en profundidad (Cisneros, 2017).

La mayor parte de las organizaciones presentan problemas de seguridad, siendo lo más importante detectarlos a tiempo (Solarte, Rosero, & del Carmen Benavides, 2015). Tradicionalmente las organizaciones establecen parámetros de seguridad para su información, entre ellos establecer un punto de control entre su red y el internet. Sin embargo, con el crecimiento que han tenido las redes y la convergencia de servicios, esta creencia ha sido totalmente desvirtuada, la mayor cantidad de los ataques a la información de una organización, no provienen de la parte externa sino desde el interior de una organización (Solarte, Rosero, & del Carmen Benavides, 2015).

Los requerimientos de seguridad que involucran las tecnologías de la información, en pocos años han obtenido un gran auge, y más aún las de carácter globalizador, la visión de nuevos horizontes que exploren más allá de las fronteras naturales, situación que ha llevado la aparición de nuevas amenazas en los sistemas informáticos. La defensa en profundidad de los sistemas de información es una defensa global y dinámica, que coordina varias líneas de defensa que cubren la profundidad del sistema (Robayo López & Rodríguez Rodríguez, 2015).

Los sistemas de información, redes de datos, sistemas operativos y la manipulación no apropiada de la información por parte de los usuarios, han hecho que cada día se presenten más opciones para los ciberdelincuentes, por ello el aseguramiento en profundidad de los sistemas operativos toma una importancia para ser proactivos limite en lo posible vulnerabilidades y evitar pérdida de información en los equipos comprometidos. Por lo anterior, es evidente que surge la necesidad de aplicar las técnicas de aseguramiento en los sistemas operativos de las empresas, para minimizar riesgos y evitar consecuencias económicas (Robayo López & Rodríguez Rodríguez, 2015).

Para que cualquier proceso de aseguramiento sea exitoso, este debe ser llevado con políticas de seguridad de alta exigencia y una adecuada capacitación, tanto para los administradores de sistema, como a para los usuarios de la red. Se entiende que no hay sistema totalmente inmune a cualquier vulnerabilidad, pero implementar este proceso es un paso muy importante en pro de la seguridad informática de cualquier organización. Defensa en profundidad (Defense in Depth) es una iniciativa que pretende aislar en capas y dividir en diferentes áreas las instalaciones con el propósito de hacer más difícil el acceso a los servidores donde se encuentra la información (Robayo López & Rodríguez Rodríguez, 2015).

Consientes que el activo más importante de una empresa son los datos. Si estos cayeran en manos de la competencia o sufrieran daños, tendríamos problemas importantes por ser custodios de información. A nivel de cliente, los datos almacenados localmente son especialmente vulnerables. Si se lograra vulnerar un equipo, es posible realizar copias de seguridad, restaurar y leer los datos en otro equipo, aunque el delincuente no pueda conectarse al sistema, es recomendable proteger los datos de varias formas, cifrado de la información, modificación de las listas de control de acceso, para evitar que el atacante llegue en forma directa a los archivos (Samper & Bolaño, 2015).

---

2. Esquema de red a implementar

La estructura de red, es considerada importante debido a que toda empresa hace uso de las TICs para de sus actividades, una red empresarial debe cumplir con un sinnúmero de requisitos, siendo la seguridad de la información lo más importante (Guo, Dong, Ren, & Huang, 2017). Cabe señalar que cuando se fortalece los esquemas de red, las empresas pueden movilizar y coordinar mejor los recursos y actividades de sus usuarios, adquirir conocimiento y absorber experiencia de cooperación. La principal causa de pérdida de beneficios económicos, está dado principalmente por fallos seguridad, haciendo que una empresa pueda perder miles de dólares al día, teniendo esto en cuenta, se ha decidido plantear un modelo o arquitectura de red que cumpla las necesidades de una empresa y que a la vez presente un esquema de seguridad que disminuya las posibles vulnerabilidades de una empresa [5, 7].

El modelo de red presentado en esta propuesta cuenta con una zona desmilitarizada (DMZ) compuesta por servidores que ofrecen los servicios WEB público y Correo, para los usuarios de la empresa en cuestión; además se ubica en otros servidores servicios para controlar de navegación (Proxy) de los empleados. También se cuenta con una red de área local (LAN) donde se alojan dos servidores con servicios de directorio activo para el control de los usuarios y la puesta en marcha de las políticas de seguridad, así como la implementación de servicios como: DHCP, DNS, WINS, y IIS para uso interno. Las terminales están conectadas a través de un Firewall que permite la salida a internet a la red LAN y DMZ para que los usuarios puedan realizar navegación web.

Tabla 1
Especificación del esquema de red empresarial.

Nombre PC	IP	Servicio	Interfaz
SRV-DC-01	192.168.1.10/24	DA/GPO, DHCP, DNS, WINS, IIS.	Ethernet
SRV-DC-02	192.168.1.11/24	DA/GPO, DHCP, DNS, WINS.	Ethernet
PC-01	192.168.1.12/24	Cliente	Ethernet -LAN
SRV-DCML-01	192.168.137.1/24	Proxy, Correo, Web público, Control de navegación	ensp01 – DMZ
SRV-DB-01	192.168.137.2/24	Base de datos	DMZ
SRV-FW-01	192.168.1.100/24	Firewall	Eth0 - WAN
	192.168.137.100/24		Eth1 - LAN
	10.0.4.15/24		Eth2 - DMZ

En esta estructura de red se consideraron convenciones de nombres como los señalados a continuación:

SRV: para referirse a un SERVIDOR.

DC: Controlador de Dominio.

01: Primer equipo.

PC: Computadora personal.

DB: Bases de Datos

FW: Firewall.

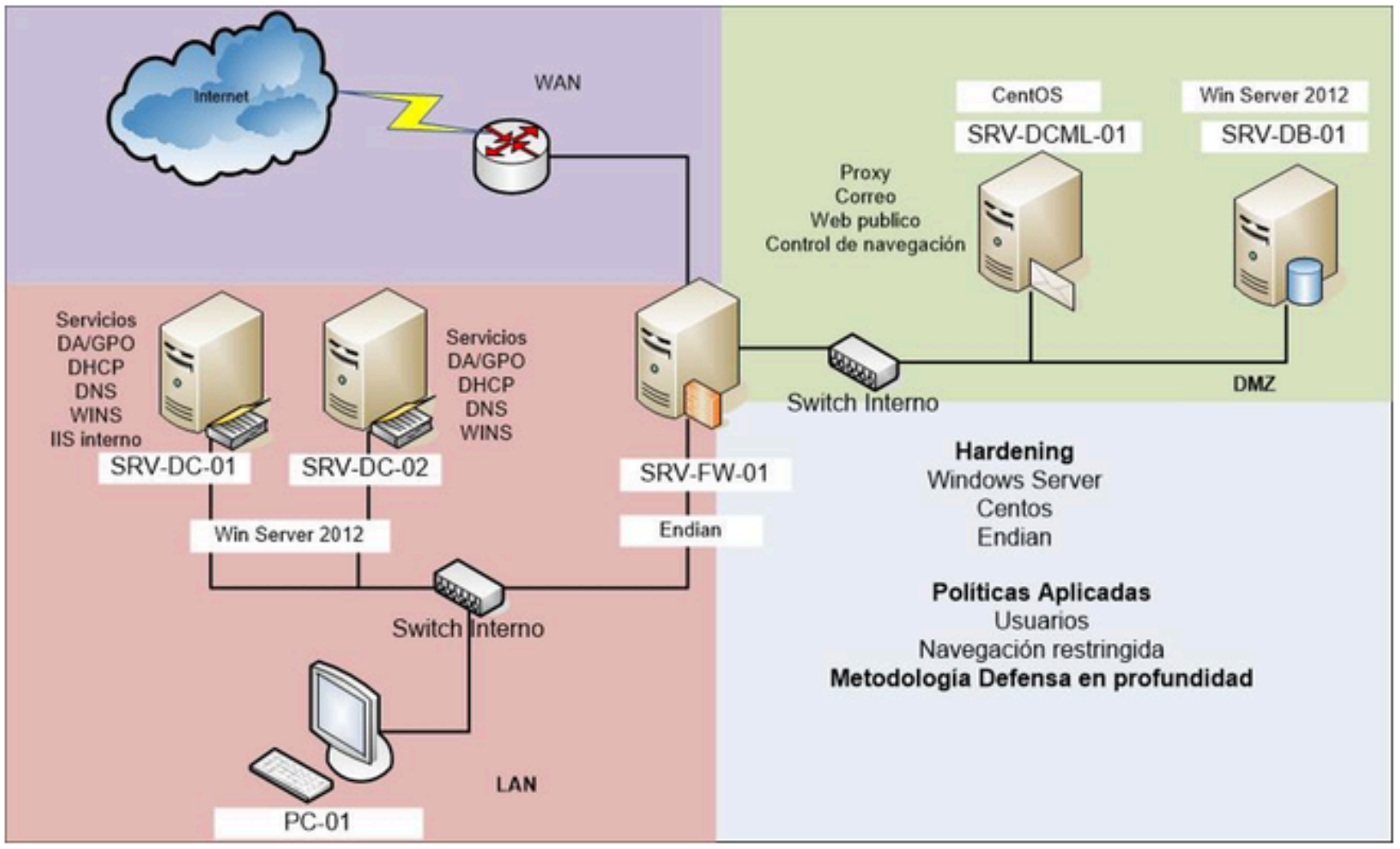
DCML: Control de Navegación, Mail, Proxy

GPO: Directivas de grupo

DNS, DHCP, WINS, IIS: servicios comúnmente usados en una estructura de red.

A continuación, la figura 1 representa la estructura de red que se diseñó para representar los esquemas de seguridad planteados en este trabajo.

Figura 1
Estructura de red empresarial



Los servidores de red, en la DMZ están distribuidos en un server con nombre SRV-DCML-01 el cual cuenta con la distribución de GNU/Linux, CentOS 7 y el otro servidor con nombre SRV-DB-01 el cual cuenta con una distribución de Windows Sever 2012 R2, la red LAN cuenta con dos servidores nombrados SRV-DC-01 y SRV-DC-02 los cuales cuentan Windows Server 2012 R2, los equipos de los usuarios de la empresa se asocian con nombres PC-01, …,PC-XX, contarán con Windows 7 Ultimate, que estará en el dominio del directorio activo del servidor SRV-DC-01 y el otro servidor estará de respaldo en caso de que el primero presente fallas, el firewall implementado es una distribución de GNU/Linux, Endian que filtrará el tráfico entre las redes LAN, DMZ, y WAN

2.1. Firewall

Un firewall, es considerado un dispositivo de capa 3 que filtra el tráfico entre 2 o más redes. En la actualidad se promueven distintos firewall siendo unos basados en hardware otros en software, pero lo que resulta importante es la forma como gestionamos el sistema operativo que permite filtrar el tráfico TCP, UDP, ICMP, IP, entre otros, lo importante es como decidir si un paquete pasa, se modifica, se convierte o se descarta. Los firewalls han constituido una primera línea de defensa en seguridad de la red durante más de 25 años. Establecen una barrera entre las redes internas protegidas y controladas en las que se puede confiar y redes externas que no son de confianza, como Internet (Cisco, 2018).

Funciona a nivel de red en la capa 3 del modelo OSI, capa 2 del stack de protocolos TCP/IP

como filtro de paquetes IP. A este nivel se pueden realizar filtros según los distintos campos de los paquetes IP: dirección IP origen, dirección IP destino. A menudo en este tipo de firewall se le permiten filtrados de varios niveles como red, transporte (capa 3 TCP/IP, capa 4 Modelo OSI), además se filtra el puerto origen y destino, a nivel de enlace de datos (no existe en TCP/IP, capa 2 Modelo OSI) como la dirección MAC (Martinez, Pacheco, & Isacc, 2009).

2.2. Proxy

Un proxy es un servicio que sirve de intermediario entre un ordenador conectado a Internet y el servidor que está accediendo. Trabaja en el nivel de aplicación (capa 7 del modelo OSI), de manera que los filtrados, se pueden adaptar a características propias de los protocolos de este nivel. Por ejemplo, si se trata de tráfico HTTP, FTP o SMTP, se pueden realizar filtrados según la URL a la que se está intentando acceder. Permite que los computadores de una organización entren a Internet de una forma controlada además oculta de manera eficaz las verdaderas direcciones de red (Martinez, Pacheco, & Isacc, 2009).

2.3. Red DMZ

En seguridad informática hace referencia a la Zona Desmilitarizada (DMZ) su origen data de la guerra fría, es una subred que está detrás del firewall pero que está abierta al público que provee servicios como WEB, EMAIL o FTP, además no puede acceder a la red LAN (GARRIDO PEÑALVER, 2017). El servidor implementado en esta propuesta es CentOS 7 a través del servicio Proxy, filtra el tráfico web de la red LAN, (cisco, 2017) expone que los defensores utilicen los proxy en el análisis de contenido para detectar amenazas potenciales que afecten la infraestructura de red, o bien, debilidades de la red que permiten a los adversarios tener acceso a las computadoras de los usuarios, entrar a las organizaciones y ejecutar sus campañas (Christian, 2017).

2.4. Red LAN

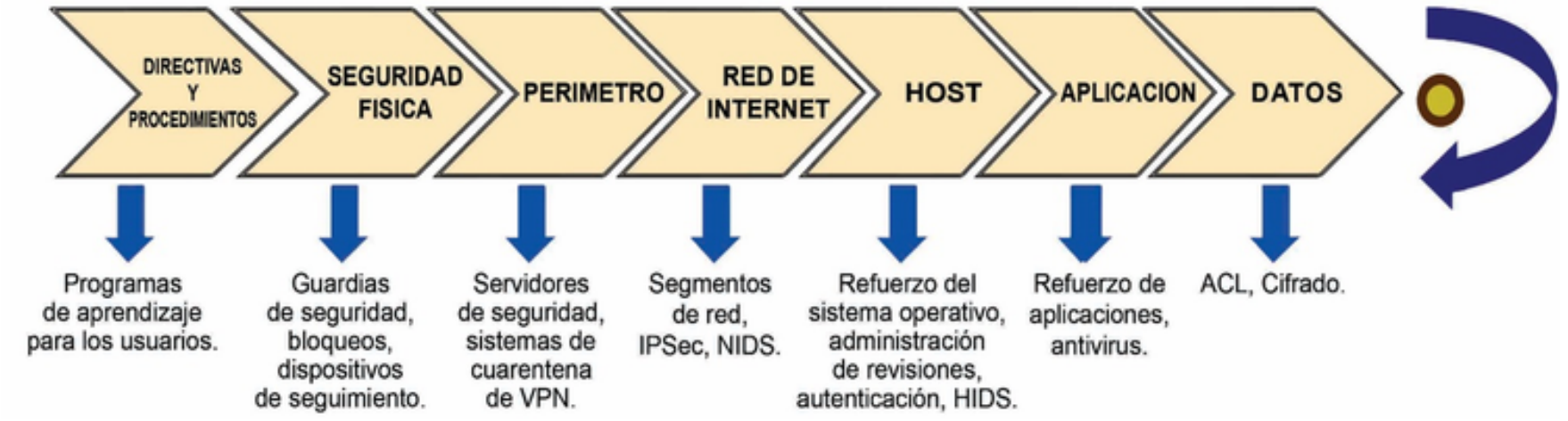
La Red de Área Local (LAN) al contar con dos servidores que proveen Directorio Activo, estos permitirán la administración de los usuarios, una vez aplicadas las políticas de seguridad a los equipos, mediante el uso de las directivas de grupo (GPO), además contarán con acceso a internet, por los servicios ofrecidos desde la DMZ, en cuanto al tráfico de red se realizan filtrados por medio del servicio de Proxy. La red empresarial, que se muestra en la Figura 1, cuenta con direccionamiento lógico basado en IPV4, tal como se muestra en la tabla 1.

---

3. Implementado defensa en profundidad en la red empresarial

La defensa en profundidad, es un método que busca disminuir las vulnerabilidades en los sistemas informáticos, la cual consiste en aplicar seguridad por capas a un sistema, su función principal es de aumentar la posibilidad de detectar intrusos y disminuir las oportunidad que los intrusos logren su propósito, la figura 2 presenta el esquema en capas de la defensa en profundidad.

Figura 2
Representación del método de defensa en profundidad por capas.



En una empresa se debe tener presente, que el activo más valioso son los datos, por esta situación se los lleva al final de la metodología para aplicar medidas de seguridad que protejan los mismos, tal como se muestra en la figura 2. Recordemos que la una vez implantadas la seguridad por capas para poder llegar a los datos se debe pasar por las capas inferiores para que así, si un posible atacante decidiera vulnerar deberá utilizar diferentes métodos para poder atravesar cada capa hasta que slos sistemas esto, le resulte más complejo y de ser posible desista, por la cantidad de barreras implementadas, esa es la esencia del método de defensa en profundidad (Cisneros, 2017).

3.1. Defensa en profundidad a capa 1

En la primera capa, se establecen las directivas a aplicar en una empresa, es decir las políticas, y procedimientos que los usuarios deben seguir en forma obligatoria para esto se analizan que recursos que debemos proteger, quienes serán los responsables, cuales son las posibles amenazas, la importancia del recurso y finalmente qué medidas se puede implementar en un servidor de seguridad.

3.2. Defensa en profundidad a capa 2

En la capa 2, se bloquean los dispositivos y se lleva un control y seguimiento de las actividades de los usuarios en los cuartos de equipos, así como la manipulación de los servidores, a través de bitácoras de uso, para esto se ubicaron en la estructura de red LAN, dos servidores con el mismo sistema operativo, en este caso Windows server 2012 R2, con los servicios de directorio activo dispuesto para implementar las directivas de grupo, a los usuarios y equipos, que a su vez las bases de datos de los usuarios, estén en continua replicación es decir, que sean redundantes de tal forma que si uno llega a fallar el otro se promueve como principal y mantenga a los usuarios conectados, claro está con los servicios necesarios para habitar esta funcionalidad.

3.3. Defensa en profundidad a capa 3

Esta capa pretende asegurar el perímetro de la red, la cual se compone de la parte externa de la red, donde el actor principal es un servidor firewall, este consta de un sistema operativo de libre distribución endian, este cubre la función de filtrar paquetes los paquetes de datos para permitir el paso o bloquear los ataques, cumpliendo las reglas planteadas en la capa 1.

Por una parte se realizó la traducción de direcciones de red (NAT- Network Address Translation) permite a una empresa disimular las configuraciones de direcciones IP y de puertos internos para impedir que los usuarios ataquen los sistemas internos con información de red robada. Los mecanismos de seguridad del perímetro pueden ocultar los servicios internos, incluso aquellos que están disponibles externamente, de modo que un intruso nunca se comunique de forma directa con ningún sistema que no sea el servidor de seguridad. Además en esta capa se implementa un servidor de seguridad SRV-FW-01 como firewall este equipo será el encargado de aplicar políticas de seguridad, para lo cual se aplican las siguientes reglas:

- Redirigir el tráfico de la red LAN por los puertos http-80, https-443 y dns-53 hacia el servidor SRV-DCML-01 proxy que está en la máquina con el sistema operativo CentOS 7.
- Permitir el tráfico desde la red LAN por los puertos MySQL-3306 que vayan hacia la red DMZ.
- Permitir el tráfico desde la red DMZ hacia la red WAN (internet) por los puertos http-80, https-443 y dns-53.
- Permitir el tráfico entre red LAN y red DMZ.
- Denegar todo el tráfico que venga desde la red WAN (internet) hacia la red LAN y la red DMZ.
- Denegar todo el tráfico.

3.4. Defensa en profundidad a capa 4

Se procedió a segmentar la red por medio de direccionamiento lógico, aplicando criterios de subredes para contribuir con la disminución de las vulnerabilidades de la red, además se diseñaron esquemas que consideran tres secciones; la red LAN, la WAN y la DMZ. Cabe señalar que para efectos didácticos, la LAN tiene asignado un segmento de red de clase C, 192.168.1.0 y máscara de subred 255.255.255.0 (/24), mientras que la DMZ tiene asignada una red 192.168.137.0 con una máscara de subred /24 y para la wan la IP que asign el proveedor, para fortalecer la seguridad de la red, se sugiere cifrar los canales por medio de IPSEC, también crear particiones para impedir que la estructura de red este disponible desde un único punto. Para proteger el entorno de la red interna, se debe requerir que cada usuario se autentique de forma segura en un controlador de dominio y en los recursos a los que tenga acceso se encuentren auditados para reducir riesgos de seguridad.

3.5. Defensa en profundidad a capa 5

Para una mayor protección en los quipo de la red LAN, se aplicaron criterios de hardening a los sistema operativo, es decir se disminuye las vulnerabilidades tanto en los cliente de red como en los servidores, se crearon sistemas de autenticación para llevar el control de los usuarios, se trabajó con certificados de seguridad a nivel de Unidades certificadoras desde el Directorio activo, el cual permite una mejor administración de los recursos de la red, en esta sección las políticas de grupo tributan directamente en el aseguramiento de la red.

Para aumentar la seguridad en los servidores se aplicaron las siguientes las siguientes políticas como base:

- Establecer el umbral de bloqueo de cuenta a 3 intentos.
- Establecer que la duración de bloqueo de cuenta en 15 minutos o más.
- Desactivar el inicio de sesión como invitado.
- Establecer la configuración del firewall por defecto, activar el perfil de dominio, privado y público.
- Bloquear los puertos USB de los equipos de la red.

Considerando estas políticas de grupos a manera de ejemplo se implementa seguridad a nivel host en el escenario propuesto y con las pruebas de validación se muestra que los ataques se reducen a nivel local y externo.

3.6 Defensa en profundidad a capa 6

En los equipos clientes, se implementa el uso de un antivirus, para ayudar a impedir la ejecución de código malicioso. Si una aplicación se ve comprometida, es posible que el intruso pueda tener acceso al sistema con los privilegios de la cuenta comprometida y los privilegios que tenga la aplicación, por tanto es necesario revisar la ejecución de los servicios y aplicaciones para que estas operen con el menor privilegio posible.

---

4. Conclusiones

La implementación de defensa en profundidad propuesta en este artículo, hace posible mitigar en forma eficaz las constantes amenazas que se dan en las redes de empresariales, de darse el caso, este puede resultar perjudicial y generar pérdidas económicas y sociales. Cabe señalar que el escenario de prueba, permitió simular ataques reales hacia una posible empresa como si fuera un hackers o un exempleados, y los resultados obtenidos revelaron

que se disminuye el nivel de efectividad del ataque son los esquemas planteados en este artículo.

Además se comprobó que los muchos de los típicos ataques fueron mitigados gracias a la presencia de un Directorio Activo, puesto que se pudo representar las políticas de grupos y evitar los ataques internos y externos.

La implementado un firewall con una red DMZ evito que la red sea expuesta en caso de un ataque externo; además se logró la mitigación de malware que provenían de la red interna por parte de los usuarios o proveniente de internet a través de páginas web maliciosas o correos con contenido no deseado. Usando el método planteado en este artículo se pudo comprobar el valor de aplicar defensa en profundidad en las redes empresariales.

4.1. Recomendaciones

Considerar que este artículo no pretende revelar el paso a paso que brinda una seguridad máxima, pero el método logra disminuir las vulnerabilidades de los datos de una empresa para (Veloz J. , Alcivar, Salvatierra, & Silva, 2017) muestran la busqueda de vulnerabilidades. Sin embargo, para un principiante el utilizar esta metodología le da buen punto de partida, para la protección de los datos, otros autores sugieren aplicar una estructura jerárquica para mejorar la seguridad de la red interna, como la creación de redes Virtuales (VLAN) (Tapia Celi, Guijarro- Rodríguez, & Viteri Guevara, 2018), finalmente se podría cifrar los medios con algoritmos propios y añadir un sistema detector de intrusos en la Red (NISD).

Referencias bibliográficas

Christian, A. (2017). SOLUCIONES OPEN SOURCE PARA SEGURIDAD PERIMETRAL DE EMPRESAS PYMES OPEN SOURCE SOLUTIONS FOR PERIMETER SAFETY FOR SMALL BUSINESSES. *UNIVERSIDAD Y CAMBIO, 2*.

cisco. (2017). *Reporte Semestral de Seguridad.*

Cisco. (2018). *cisco*. Obtenido de cisco: https://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html

Cisneros, C. I. (2017). MODELO DE SEGURIDAD DE DEFENSA EN PROFUNDIDAD PARA LOS GADS (GOBIERNOS AUTONOMOS DESCENTRALIZADOS) MUNICIPALES DEL ECUADOR CON BASE EN EL SISTEMA DE GESTIÓN DE INFORMACIÓN. *(Master's thesis)*.

GARRIDO PEÑALVER, V. (2017). Diseño, Implementaci ón y Validación de un Cyber Range.

Guo, T., Dong, J., Ren, X., & Huang, Y. (2017). The Core Enterprise Network Competence, Network Characteristics and the Innovation Network Governance Performance–From Chinese Microcosmic Evidence. *Eurasia Journal of Mathematics, Science and Technology Education, 13*(12), 7823-7833.

Martinez, k., Pacheco, J., & Isacc, Z. (2009). Firewall, una solución de seguridad informática. *RUI - Rev. UIS Ingeniería.*, 20-22.

Muñoz, M., & Rivas, L. (2015). Estado actual de equipos de respuesta a incidentes de seguridad informática. *RISTI-Revista Ibérica de Sistemas e Tecnologías de Informação*, 1-15.

Robayo López, J., & Rodríguez Rodríguez, R. (2015). Aseguramiento de los sistemas computacionales de la empresa. *Sitiosdima. net*.

Samper, J., & Bolaño, M. (2015). Seguridad informática en el siglo xx: una perspectiva jurídica tecnológica enfocada hacia las organizaciones nacionales y mundiales. *Publicaciones e Investigación, 9*, 153-162.

Solarte, F. N., Rosero, E. R., & del Carmen Benavides, M. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica-ESPOL, 28*(5).

Tapia Celi, J., Guijarro- Rodríguez, A., & Viteri Guevara, X. (2018). Práctica de aplicación de

seguridad y distribución de LAN corporativa. *Universidad y Sociedad, 10*(1), 41-45.

Veloz, J., Alcivar, A., Salvatierra, G., & Silva, C. (2017). Ethical hacking, una metodología para descubrir fallas de seguridad en sistemas informáticos mediante la herramienta Kali-Linux. *REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS COMUNICACIONES, 1*(1), 1-12.

---

1. Master Universitario en Modelado Computacional de Ingeniería por la Universidad de Cádiz, Ingeniero en Computación por la Escuela Superior Politécnica del Litoral, Ecuador, Profesor de la Facultad de Ciencias Matemáticas y Físicas, Universidad. de Guayaquil, alfonso.guijarror@ug.edu.ec

2. Magister Universitaria en Contabilidad y Auditoría en la Universidad Laica Vicente Rocafuerte, Magister en Docencia y Gerencia en Educación Superior por la Universidad de Guayaquil, Ingeniera Comercial por la Universidad de Guayaquil, Docente de la Facultad de Ciencias Matemáticas y Física, Universidad de Guayaquil, jessica.yepezh@ug.edu.ec

3. Magister en Docencia y Gerencia en Educación Superior, Ingeniero en Sistemas Computacionales, por la Universidad de Guayaquil, Profesora de la Facultad de Ciencias Matemáticas y Físicas, Universidad. de Guayaquil, tania.peraltag@ug.edu.ec

4. Master en Administración Pública por la Universidad Tecnológica América de Guayaquil-Ecuador, Abogada de los Tribunales de la República del Ecuador por la Universidad de Guayaquil, Ecuador, Profesora de la Facultad de Ciencias Matemáticas y Físicas, Universidad. de Guayaquil, mirella.ortizz@ug.edu.ec

---

Revista ESPACIOS. ISSN 0798 1015
Vol. 39 (Nº 42) Año 2018

[Índice]

[En caso de encontrar un error en esta página notificar a webmaster]