Conceptos básicos de seguridad informática y sus generalidades

Ezaleth Emith Serrano
Universidad Nacional Abierta y a Distancia "UNAD"

***Resumen*— En este documento se describen algunos conceptos importantes para entender la aplicación de la seguridad informática, de forma que, entendiendo su conceptualización, se facilite la implementación de herramientas que minimicen las vulnerabilidades que los mantiene expuestos. Temas como zonas DMZ, ley de delitos informáticos y aplicaciones UTM, son algunos de los temas tratados expuestos a continuación.**

***Palabras clave*— DMZ. UTM, seguridad informática, puertos, certificaciones.**

***Abstract*— This document describes some important concepts to understand the application of computer security, so that understanding its conceptualization, facilitate the implementation of tools that minimize the vulnerabilities that keep them exposed. Topics such as DMZ zones, cybercrime law and UTM applications are some of the topics discussed below.**

***Keywords*— DMZ. UTM, computer security, ports, certifications.**

I. INTRODUCCIÓN

A través de la selección y aplicación de candados o protecciones, la seguridad ayuda en la misión de la organización por la protección de sus recursos físicos y financieros, la reputación, la posición legal, empleados y otros activos tangibles e intangibles. Para muchos, la seguridad es a veces vista como frustrar los objetivos de negocio, mediante la imposición de normas y procedimientos que causan molestia a los usuarios, administradores, y los sistemas. Estas normas y procedimientos de seguridad no son elegidos no existen por comodidad, sino que se ponen en marcha para proteger los activos importantes y por lo tanto apoyar los objetivos de negocio.

Proporcionar una protección eficaz de la información requiere un enfoque global que tenga en cuenta una variedad de áreas, tanto dentro como fuera del área de tecnología de la información. Un programa de protección de la información es más que el establecimiento de controles para los datos almacenados en una computadora. En 1965 se introdujo por primera vez el concepto de "oficina sin papeles". La llegada de la tercera generación de computadoras trajo a la luz este concepto. Sin embargo, hoy en día la mayor parte de toda la información disponible para los empleados y otros todavía se encuentra en forma impresa. Así que, para ser un programa eficaz, la protección de la información debe ir más allá del pequeño ámbito de las Tecnologías de Información y abordar las cuestiones de protección de la información en toda la empresa. Un programa integral debe tocar todas las etapas del ciclo de vida de los activos de información desde la creación hasta la destrucción final. [1]

II. ACTIVIDADES

1. Listado de puertos y funciones para prestar el servicio de correo.

Los clientes de correo electrónico utilizan diferentes protocolos de servicio, por tanto, hay funcionamientos y puertos disponibles para tal efecto. Por ejemplo, como se muestra en la figura 1, donde se tienen los puertos y protocolos usados por la herramienta Exchange de Microsoft. [2]

Los puertos 25 y 587 se utilizan para proporcionar la conectividad del cliente con el servicio de transporte en la parte delantera de la función de servidor de acceso de cliente (CAS) en SMTP.

Puerto 465 es utilizado por el servicio de transporte de buzón de correo para recibir las conexiones de cliente proxy de la función CAS en SMTP de forma segura (SMTPS).

Puerto 475 es utilizado por la función de buzón para comunicarse directamente con otras funciones de buzón, la transferencia de correo entre el servicio de envío de transporte de buzón de correo y el servicio de entrega de transporte buzón.

El puerto 2525 se utiliza por la función de buzón de SMTP desde el servicio de transporte de extremo delantero del CAS, mientras que continúa para utilizar el puerto 25.

Servidor de correo POP3 escucha por el puerto 110 TCP.

El puerto 587 es utilizado como puerto alternativo al 25 para correo de salida con SMTP.

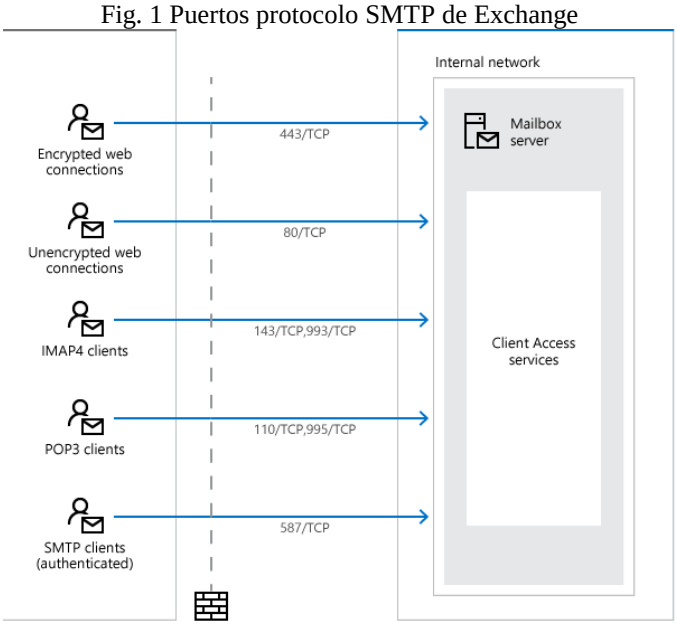
Puerto de entrada de correo POP3 sobre SSL usado por Gmail.

Puerto 143 es usado por el servidor de correo IMAP.

Puerto 993 de entrada de correo SMTP sobre SSL.

Puerto 220 es alternativo para correo IMAP. [3]

Fig. 1 Puertos protocolo SMTP de Exchange



2. Certificaciones enfocadas a la seguridad informática, que contiene y el costo de las mismas.

2.1. CompTIA Security+:

Es una organización creada con el objetivo de desarrollar y promover certificaciones IT independientes de los fabricantes. El examen certifica que se tengan los conocimientos en:

- Cryptography
- Identity Management
- Security Systems
- Organizational Systems
- Security Risk Identification and Mitigation
- Network Access Control
- Security Infrastructure

El costo es de 320.00 USD y a partir del 2011 hay que renovarla cada 3 años.

2.2 CEH: Certified Ethical Hacking

La certificación CEH Ethical Hacking prepara al profesional de IT para que piense y actúe como un Hacker, utilizando las mismas herramientas de hacking, mid-set y técnicas que utilizaría un Hacker al momento de violar la seguridad de una red. Esta certificación cumple con la filosofía de "para vencer a tu enemigo debes primero conocerlo"

Es una certificación que se ha convertido en necesaria para las personas que quieren ser Hacker ético. El profesional que obtiene la certificación CEH Ethical Hacking posee habilidades y conocimientos en las siguientes áreas:

- Foot printing and Reconnaissance
- Scanning Networks
- Enumeration
- System Hacking
- Trojans
- Worms
- Virus
- Sniffers
- Denial of Service Attacks
- Social Engineering
- Session Hijacking
- Hacking Web Servers
- Wireless Networks
- Web Applications
- SQL Injection
- Cryptography
- Penetration Testing
- Evading IDS
- Firewall and Honeypots

El costo de la certificación es de 500.00 USD.

2.3 Cisco CCNA Security

Cisco CCNA Security es una certificación de seguridad Entry Level orientada a soluciones Cisco. El profesional que obtiene la certificación Cisco CCNA Security posee habilidades y conocimientos en las siguientes áreas:

- Common Security Threats
- Security and Cisco Routers
- AAA on Cisco Devices
- IOS ACLs
- Secure Network Management and Reporting
- Common Layer 2 Attack
- Cisco Firewall Technology
- Cisco IPS

La certificación cuenta con preguntas de selección múltiple y simulaciones. El costo es de 500.00 USD.[4]

2.4 CISSP: Certified Information System Security Professional

CISSP es una certificación avanzada en seguridad orientada aquellos profesionales que quieren seriamente hacer una carrera como especialistas. Esta certificación es independiente de fabricantes y es ofertada por el International Information Systems Security Certification Consortium, conocida también como (ISC)2.

Los dominios son:

- Information Security and Risk Management
- Access Control
- Cryptography
- Physical Security
- Security Architecture and Design
- Legal, Regulations, Compliance, and Investigation
- Telecommunications and Network Security
- Business Continuity and Disaster Recovery Planning
- Applications Security
- Operations Security

Para obtener la certificación CISSP el candidato debe aprobar el examen que tiene un costo de 599.00 USD. Cada examen de concentración tiene un costo de 399.00 USD.

2.5 CISM (Certified Information Security Management)

El CISM es el estándar aceptado globalmente para las personas que diseñan, construyen y gestionan los programas de seguridad de la información empresarial. CISM es la principal certificación para administradores de seguridad de la información. El último índice trimestral de valoración de Habilidades y Certificaciones IT (ITSCPI) de Foote Partners clasificó a CISM como la más codiciada y la que más se paga de las certificaciones de seguridad.

El examen está dividido en 5 áreas:

- Gobierno de la seguridad de la información
- Administración de riesgos de información
- Desarrollo de un programa de seguridad de información
- Administración del programa de seguridad de información
- Manejo y respuesta de incidentes

El costo de la certificación es de 675.00 USD.

2.6 GSEC: Essential SANS GIAC Security

Los que posean las certificaciones gsec demuestran conocimientos y habilidades técnicas en áreas tales como:

- Protocolos de Wi-Fi
- La identificación y prevención de ataques comunes e inalámbricas
- La cartografía de la red
- Conmutación de redes de telefonía pública
- Controles de acceso
- Autenticación
- Administración de contraseñas
- DNS
- Fundamentos de criptografía
- ICMP
- IPv6
- Infraestructura de clave pública
- Linux
- Mapeo de red
- Protocolos de red

El costo de la certificación es de 1099 USD.[5]

3. Redactar la conceptualización de qué es una DMZ, sus componentes, ¿cómo se organiza una DMZ? El estudiante deberá generar un gráfico para describir la DMZ.

Uno de los mecanismos de defensa para proteger la información de la empresa es la instalación de Firewalls. Lo que esto hace es definir reglas de acceso entre dos redes: la interna y la externa.

Sin embargo, no todas las subredes tienen las mismas políticas de seguridad pues, en ocasiones, puede presentarse el escenario en que sea necesario acceder a equipos de la red interna, desde afuera. Es allí donde surge la necesidad de aislar diferentes redes de la empresa y aparece el término de "de-militarized zone" (zona desmilitarizada) que hace referencia a una zona aislada que aloja aplicaciones a disposición del público. El DMZ sirve como una zona intermedia entre la red a proteger y la red hostil. [6]

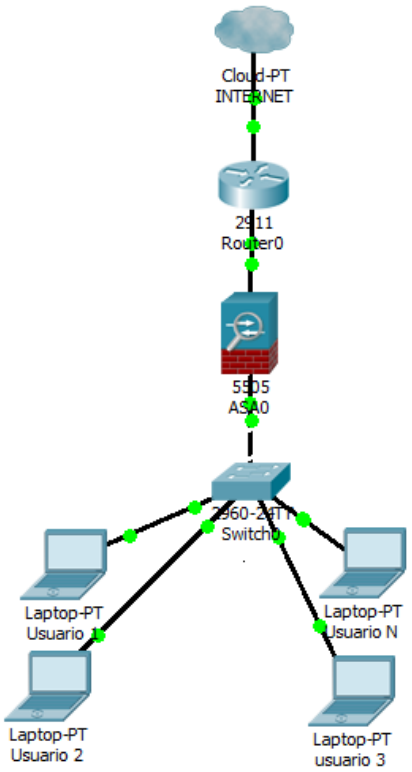
Los servidores situados en la DMZ, normalmente es la siguiente:

- Tráfico de la red externa hacia la DMZ autorizada
- Tráfico de la red externa hacia la red interna prohibida
- Tráfico de la red interna hacia la DMZ autorizada
- Tráfico de la red interna hacia la red externa autorizada
- Tráfico de la DMZ hacia la red interna prohibida
- Tráfico de la DMZ hacia la red externa rechazada.

Dado que se tiene acceso desde la red externa, no tiene un nivel de protección muy alto, por lo que no es recomendable almacenar datos críticos de la empresa.

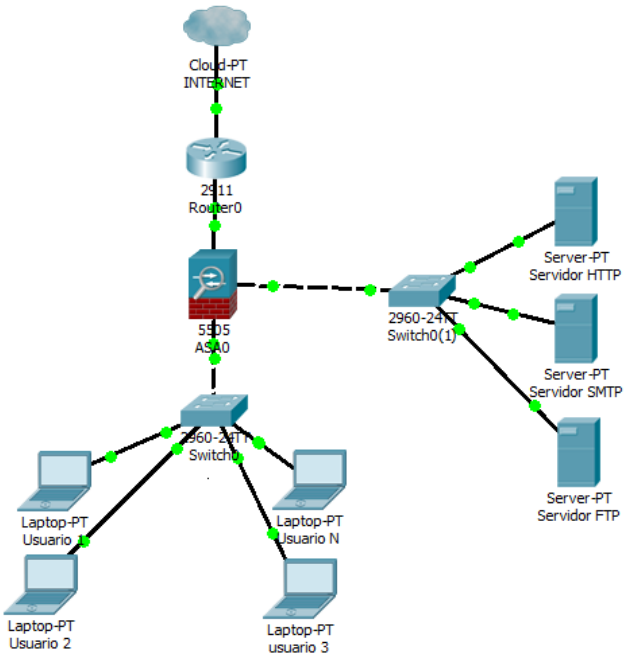
Las configuraciones de red, de forma general, de una empresa, presenta una arquitectura con un router que conecta la red interna con la red externa, un firewall para la protección de la intranet; un switch para la conexión de los equipos y por último los usuarios, como se presenta en la figura 2.

Fig. 2 Representación de una red sin DMZ



Ahora, una red con una DMZ, adicional a los equipos anteriormente mencionados, requiere un switch más; esto con el fin de poder conectar al firewall por otra rama los equipos que hacen parte de esta subred, como se muestra en la figura 3.

Fig. 3 Representación de una red con DMZ



4. Elementos informáticos más importantes en una organización que cuenta con una Intranet y que el acceso se proyecta a través de un DMZ, elementos Hardware y software que se deben configurar para generar una seguridad adecuada en la organización, marcas de equipos, aproximación de costos por equipo.

Los elementos más importantes para una empresa que desea implementar la intranet con el acceso proyectado por la DMZ son 5 principalmente:

- Sistema operativo residente en cliente y servidor
- Router con firewall integrado
- Switches
- Servidor(es)
- Equipos usuarios

Uno de los sistemas operativos más usados a nivel general es Windows, por tanto, utilizar un servidor web que sea compatible con este es lo ideal. Se tiene la opción de Microsoft IIS que corre sobre la misma plataforma y su descarga no tiene costo; además se ejecuta en el servidor de producción y es compatibles con versiones a partir de XP. [7]

Por otro lado, una de las marcas más reconocidas en el campo de las comunicaciones es Cisco, quien presenta una buena opción para la aplicación de estudio con un router 4331 con funciones de Firewall integrada. El precio de este equipo en Amazon, está en promedio en USD $1450.00.

De la misma forma, los switches son necesarios para la conexión de los equipos de las subredes, y en este caso, como se tiene un DMZ, se deben utilizar dos de ellos.

Para la red LAN se debe usar un equipo capa 2 con funciones capa 3, para el enrutamiento de los puertos, por tanto, se tiene como opción un Cisco Nexus 3548, que tiene un costo promedio de USD $6845.00 en la plataforma Amazon. El switch capa 2 que se ubica en la DMZ es un switch Cisco Catalyst 2960, que, en la misma página de ventas, está en USD $ 1581.00.

Para los servidores, aunque existen muchas posibilidades y la mayoría son buenas, la marca Thinkpad de Lenovo es una línea empresarial hecha para trabajos pesados. Por tanto, una buena opción es un Lenovo System x3100 con 8 Gb de RAM expandible a 32, un procesador Intel Xenon de 3,1 GHz, disco duro de 1 Tb de almacenamiento y 7200 rpm. El costo de este es de USD $799.99.

Los equipos finales pueden ser cualquier tipo de pc que tenga forma de conectarse a la red local. Siguiendo la misma línea del servidor, equipos portátiles Thinkpad, con 8 Gb de RAM y 500 Gb de almacenamiento tienen un precio promedio de USD $640 y equipos de escritorio con características similares, USD $409.

5. ¿Qué es una UTM? ¿Por qué sería importante aplicar una UTM a una organización, qué problema podría tener el aplicar una UTM? ¿Cómo mitigar el impacto negativo que trae consigo la UTM?

Unified threat management, que significa Gestión unificada de amenazas y se abrevia como UTM, es un término de seguridad de la información que se refiere a un único dispositivo de seguridad que proporciona múltiples funciones en un único punto de red. Normalmente incluye funciones como:

- antivirus
- antispyware
- anti spam
- firewalls
- detección y prevención de intrusiones
- filtrado de contenido y prevención de fugas.

Algunos también ofrecen servicio de enrutamiento remoto, traducción de direcciones de red NAT y soporte de redes privadas virtuales VPN. [8]

Esta solución se hace atractiva al cliente por la simplicidad de la misma, pues no es necesario tener un proveedor de cada uno de los servicios anteriormente mencionados, sino que en un solo equipo o segmento de red se concentran todas y se ejecutan a través de una consola.

Estos equipos han ganado fuerza en la industria, dado que han ido apareciendo amenazas que son combinaciones de diferentes tipos de malware y ataques que son dirigidos de forma simultánea a diferentes partes de la red y tener dispositivos independientes de gestión de estas amenazas, dificulta la prevención, pues cada aspecto debe gestionarse y actualizarse individualmente para mantenerse actualizado ante las ultimas formas de malware y delitos cibernéticos.

Sin embargo, aunque las soluciones de gestión unificadas solucionan algunos problemas de seguridad, también presentan otras desventajas para la red, siendo el principal, que tener un único punto de defensa de la red, también crea un único punto de fallo de la misma. Es por esto, que las organizaciones que optan por esta solución, complementan su dispositivo UTM con un software para detener cualquier malware que haya pasado por o alrededor del Firewall UTM.

Los UTM de Cisco son diseñados para redes pequeñas. El modelo Meraki X64 tiene una capacidad de máximo 50 clientes como recomendación y presenta herramientas como organización de tráfico y visibilidad de capa 7, soporte de hasta 4 SSIDs y autoconfiguración de site-to-site VPN. El costo de este dispositivo es de USD $615.37. [9]

6. Aspectos generales de la ley 1273 de 2009 delitos informáticos en Colombia, ¿cuáles son los delitos más comunes en Colombia?

La ley 1273 que se aprobó en 2009, creó nuevos tipos penales relacionados con delitos informáticos y la protección de la información y de los datos, con penas que van hasta 10 años en prisión y multas que pueden llegar a los 1500 salarios mínimos legales mensuales vigentes.

El 5 de enero de ese año, el congreso de la Republica de Colombia, promulgó la ley 1273 "Por medio de la cual se modifica el código Penal y se crea un nuevo bien jurídico tutelado, denominado "De la protección de la información y de los datos" y se preservan integralmente los sistemas los sistemas de información y las comunicaciones, entre otras disposiciones".

Dicha ley calificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las empresas se blinden jurídicamente para evitar incurrir en alguno de estos tipos penales.

Se destacan a los que ellos llamaron atentados informáticos y otras infracciones, tales como:

- Acceso abusivo a un sistema informático
- Transferencia no consentida de activos
- Hurto por medios informáticos y semejantes
- Suplantación de sitios web para capturar datos personales violación de los datos personales
- Uso de software malicioso
- Daño informático
- Interceptación de los daños informáticos
- Obstaculización ilegitima de sistema informático o red de telecomunicaciones

Lo anterior, teniendo en cuenta los perjuicios patrimoniales a los que se pueden enfrentar los empleadores debido al uso inadecuado de la información por parte de sus trabajadores y demás contratistas. Pero más allá de esto, con la aprobación de esta ley se genera una herramienta importante para denunciar los hechos delictivos que puedan afectarlo, pues anterior a ella, las empresas no denunciaban estos hechos, no solo para evitar dañar su reputación sino también porque no existían herramientas especiales que los respaldaran.

Los delitos informáticos más comunes en Colombia, según el ministerio de defensa nacional, son los siguientes:

• *Divulgación indebida de contenidos:* Son conductas originadas en el anonimato ofrecido en internet y el acceso público sin control desde cafés internet; entre ellas se encuentran el envío de correos electrónicos anónimos con fines de extorsión, amenazas, calumnias o denigración del buen nombre de las personas.

• *Violación de los Derechos de autor:* Utilizando reproductores en serie, los delincuentes realizan múltiples copias de obras musicales, videos, películas y software.

• *Estafas a través de subastas en línea:* Estas se presentan en el servicio de venta de productos, generalmente ilícitos, en línea o en la red; se pueden encontrar celulares hurtados, software de aplicaciones ilegales, además puede ser una vía de estafa ya que se suelen incumplir reglas de envió y de calidad de los productos solicitados.

• *Piratería En Internet*: Implica la utilización de internet para vender o distribuir programas informáticos protegidos por las leyes de la propiedad intelectual. Son tales como la utilización de tecnología par a par, correos electrónicos; grupos de noticias, chat por retardos de internet, orden postal o sitios de subastas, protocolos de transferencia de archivos, entre otros.

• *Claves Programáticas Espías*: Más conocidas como troyanos, o software espías, utilizadas para sustraer información en forma remota y física, preferiblemente aquella que le permita al delincuente validarse en el sistema bancario, suplantando a la víctima y obteniendo dinero de ello.

III. CONCLUSIONES

La exposición de los sistemas informáticos en una característica que se presenta en todas las infraestructuras de datos que existen; unas en mayor proporción que las otras, pero ninguna con un riesgo cero. Por tanto, es importante generar planes de desarrollo que incluyan seguridad informática, a fin de evaluar los vacíos de seguridad que puedan existir, tanto en los dispositivos de red que posean, como en las personas que hacen parte del a organización.

Es importante destacar que no siempre los vacíos en seguridad se presentan por fallas en las configuraciones, sino que algunos son inherentes de los protocolos y las tecnologías implementadas, además, algunas ocasiones, creadas por el mismo personal interno de la misma. Es por esto mismo que se deben evaluar constantemente los sistemas, a fin de minimizar riesgos y corregir los errores al máximo posible.

IV. REFERENCIAS

[1] IBM. Fundamentos de seguridad informática. [En línea] Disponible en: https://www.ibm.com/developerworks/community/files/basic/.../api/.../media.

[2] Puertos de red para clientes y flujo de correo en Exchange 2016. [En línea]. Disponible en: https://technet.microsoft.com/es-es/library/bb331973(v=exchg.160).aspx

[3] Búsqueda de puertos TCP/ UDP. [En línea]. Disponible en: http://es.adminsub.net/tcp-udp-port-finder/465

[4] CISCO. Net Working Academy. [En línea]. Disponible en: https://www.netacad.com/es/

[5] Capacity. Las 4 mejores certificaciones de Seguridad para TI en 2015. [En línea]. Disponible en: http://blog.capacityacademy.com/2014/11/04/las-4-mejores-certificaciones-de-seguridad-ti-para-2015/

[6] Redes Zone. DMZ: que es, ara que sirve y como utilizarlo. [En línea]. Disponible en: https://www.redeszone.net/2017/01/17/dmz-routers-descubre-mejor-forma-utilizacion/

[7] Internet. Intranet. Extranet. [En línea]. Disponible en: http://test.esupcom.unr.edu.ar/bv_tics/biblioteca/apuntes_catedra/apuntes/tercero_internet.pdf

[8] ¿Qué es la gestión unificada de amenazas? [En línea]. Disponible en: https://latam.kaspersky.com/resource-center/definitions/utm

[9] Amazon. https://www.amazon.com/Cisco-Meraki-Security-Appliance-200Mbps/dp/B00T8A2646

[10] Ley 1273 de 2009, disponible en: http://www.mintic.gov.co/portal/604/w3-article-3705.html