Técnicas de Seguridad

Seguridad en redes de área local.

Una **red de área local (LAN)** está diseñada para conectar computadoras personales y otros dispositivos digitales dentro de un radio de media milla o 500 metros. Por lo general, las LAN conectan unas cuantas computadoras en una pequeña oficina, todas las computadoras en un edificio o todas en varios edificios en cercana proximidad. Las LAN también se utilizan para vincularse a redes de área amplia de larga distancia (WAN, que describiremos más adelante en esta sección) y a otras redes alrededor del mundo por medio de Internet.

Recordemos que una red ésta conformada de computadoras y un switch o un hub que actúa como un punto de conexión entre las computadoras. Los **hubs** son dispositivos muy simples que conectan componentes de red, para lo cual envían un paquete de datos a todos los demás dispositivos conectados. Un **switch** tiene mayor funcionalidad que un hub y puede tanto **filtrar como reenviar datos** a un destino especificado en la red. por tanto si todavía hay hub's en la rede **deben ser sustituidos por los switchs.**

¿Y qué hay si se desea comunicar con otra red, como Internet? Necesitaría un **router** o **enrutador**: un procesador de comunicaciones que se utiliza para enrutar paquetes de datos a través de distintas redes y asegurar que los datos enviados lleguen a la dirección correcta.

Algunas técnicas de seguridad para redes LAN

1. Software antivirus, antimalware y antispyware
Los planes de tecnología defensivos tanto para individuos como para empresas deben contar con protección antivirus para cada computadora. El **software antimalware, antivirus y antispyware** están diseñados para revisar los sistemas computacionales y las unidades en busca de la presencia de virus de computadora. Por lo general, el software elimina el virus del área infectada. Sin embargo, la mayoría del software antivirus es efectivo sólo contra virus que ya se conocían a la hora de escribir el software. Para que siga siendo efectivo, hay que actualizar el software antivirus en forma continua. Hay productos antivirus disponibles para muchos tipos distintos de dispositivos móviles y de bolsillo además de los servidores, las estaciones de trabajo y las PC de escritorio.

Los principales distribuidores de software antivirus, como **Norton, McAfee, Symantec y Trend Micro, ESET** han mejorado sus productos para incluir protección contra spyware, malware.

Pero debemos tener mucho cuidado ya que existen en la internet programas de seguridad falso conocidos como **rouge**
Los códigos maliciosos del tipo rogue componen parte del ecosistema que actualmente, y económicamente hablando, forman parte del negocio del crimeware; contando en la actualidad con un importante volumen de familias que día a día inundan Internet con nuevas variantes. A continuación les dejo un nuevo y breve listado del rogue más relevante este articulo es del 2010 pero algunos siguen existiendo.

Antivirus Doctor
Anti-Virus Elite 2010
Anti-Virus Live 2010
Contraviro
Doctor Alex
Ecology Green PC
ErrorClean
Green AV
Home Antivirus 2010
Malware Mechanic
MicroV3
MicroVaccine
NoAdware
NoMalware
PC Antispyware 2010
PC Security 2009
Pope Green Defender
Privacy Center
Proof Defender 2009
Registry Doktor 2009
SaferScan
Safety Anti-Spyware
Save Defender
Save Soldier
Screen-Spy
Soft Safeness
System Cleaner
Trust Warrior
UnVirex
Windows System Suite

ESET NOD32 detecta proactivamente todas estas amenazas. Por lo tanto, lo recomendable es la implementación de una solución de seguridad **antimalware** que permita mantener la seguridad del sistema de forma eficaz.

2. Firewalles

Para **controlar el estado de los puertos de conexión a redes TCP/IP**, y por tanto de las aplicaciones que los usan, emplearemos un Firewall (**cortafuego)**.
Un **contrafuego** (***firewall*** en inglés) es una parte de un sistema o una red que está diseñada para **bloquear el acceso no autorizado**, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo hardware o software, o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios. Los cortafuegos pueden ser **implementados en hardware o software**, o una combinación de ambos. Los cortafuegos se utilizan con frecuencia para **evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas** conectadas a Internet, especialmente intranets. Todos los mensajes que entren o salgan de la intranet pasan a través del cortafuegos, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados.

Existen varias **tecnologías de filtrado de firewall**, como el filtrado de paquete estático, la inspección con estado, la Traducción de direcciones de red (NAT) y el filtrado de proxy de aplicación. Se utilizan con frecuencia en combinación para proveer protección de firewall.

El *filtrado de paquetes* examina ciertos campos en los encabezados de los paquetes de datos que van y vienen entre la red de confianza e Internet; se examinan paquetes individuales aislados. Esta tecnología de filtrado puede pasar por alto muchos tipos de ataques.

La *inspección con estado* provee una seguridad adicional al determinar si los paquetes forman parte de un diálogo continuo entre un emisor y un receptor. Establece tablas de estado para rastrear la información a través de varios paquetes. Los paquetes se aceptan o rechazan con base en si forman o no parte de una conversación aprobada, o si tratan o no de establecer una conexión legítima.

La *traducción de direcciones de red (NAT)* puede proveer otra capa de protección cuando se emplean el filtrado de paquetes estáticos y la inspección con estado. NAT oculta las direcciones IP de la(s) computadora(s) host interna(s) de la organización para evitar que los programas husmeadores, que están fuera del firewall, las puedan descubrir y utilicen esa información para penetrar en los sistemas internos.

El *filtrado de proxy de aplicación* examina el contenido de los paquetes relacionado con aplicaciones. Un servidor proxy detiene los paquetes de datos que se originan fuera de la organización, los inspecciona y pasa un proxy al otro lado del firewall. Si un usuario que esté fuera de la compañía desea comunicarse con un usuario dentro de la organización, el usuario externo primero "habla" con la aplicación proxy y ésta se comunica con la computadora interna de la firma. De igual forma, un usuario de computadora dentro de la organización tiene que pasar por un proxy para hablar con las computadoras en el exterior

Ventajas de un cortafuegos:

- **Proteger de intrusiones.** El acceso a ciertos segmentos de la red de una organización sólo se permite desde máquinas autorizadas de otros segmentos de la organización o de Internet.
- **Protección de información privada.** Permite definir distintos niveles de acceso a la información, de manera que en una organización cada grupo de usuarios definido tenga acceso sólo a los servicios e información que le son estrictamente necesarios.
- **Optimización de acceso.** Identifica los elementos de la red internos y optimiza que la comunicación entre ellos sea más directa. Esto ayuda a reconfigurar los parámetros de seguridad.

Limitaciones de un cortafuegos Las limitaciones se desprenden de la misma definición del cortafuegos: filtro de tráfico. Cualquier tipo de ataque informático que use tráfico aceptado por el cortafuegos (por usar puertos TCP abiertos expresamente, por ejemplo) o que sencillamente no use la red, seguirá constituyendo una amenaza.

Políticas del cortafuegos **.** Hay dos políticas básicas en la configuración de un cortafuegos que cambian radicalmente la filosofía fundamental de la seguridad en la organización:

Política restrictiva: se deniega todo el tráfico excepto el que está explícitamente permitido. El cortafuegos obstruye todo el tráfico y hay que habilitar expresamente el tráfico de los servicios que se necesiten.

Política permisiva: se permite todo el tráfico excepto el que esté explícitamente denegado. Cada servicio potencialmente peligroso necesitará ser aislado básicamente caso por caso, mientras que el resto del tráfico no será filtrado.
La **política restrictiva es la más segura**, ya que es más difícil permitir por error tráfico potencialmente peligroso, mientras que en la política permisiva es posible que no se haya contemplado algún caso de tráfico peligroso y sea permitido por omisión.

3. Listas de control de acceso (acl) y filtrado de paquetes

Una **Lista de Control de Acceso** o **ACL** (del inglés, ***Access Control List***) es un concepto de seguridad informática usado para fomentar la separación de privilegios. Es una forma de determinar los permisos de acceso apropiados a un determinado objeto, dependiendo de ciertos aspectos del proceso que hace el pedido.

Las ACL permiten **controlar el flujo del tráfico en equipos de redes, tales como routers y switches**. Su principal objetivo es filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo a alguna condición. Sin embargo, también tienen usos adicionales, como por ejemplo, distinguir tráfico prioritario.
Las listas de acceso de control pueden configurarse generalmente para controlar tráfico entrante y saliente y en este contexto son **similares a un cortafuegos**. Se pueden considerar como **cada una de las reglas**

Acl en routers
Para el caso de los **routers** (en el caso concreto de los *routers* de la compañía líder CISCO) las ACL son listas de condiciones que se aplican al tráfico que viaja a través de una interfaz del router, y se crean según el protocolo, la dirección o el puerto a filtrar. Estas listas indican al router qué tipos de paquetes se deben aceptar o rechazar en las interfaces del router, ya sea a la entrada de la interfaz
o a la salida. Razones principales para crear las ACL:

- Limitar el tráfico de la red.
- Mejorar su rendimiento de la red.
- Controlar el flujo de tráfico, decidiendo qué tráfico se bloquea y cuál se permite, ya sea por direccionamiento o por servicios de red.
- Proporcionar un **nivel básico de seguridad** para el uso de la red.

4. Limite la dirección del tráfico en algunos puertos, Limite algunos protocolos de red; por ejemplo, ping, SNMP.

El Protocolo simple de administración de red **SNMP** (delinglés*Simple Network Management Protocol*) es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red.
Las mejoras de la seguridad fueron promulgadas en la versión SNMPv3 por lo que es preferible usara este protocolo ya que incluye encriptación, chequeo de integridad,servicis de autenticación.
Debido a que **SNMP está diseñado para permitir a los administradores monitorear y configurar dispositivos de red de manera remota**, también se **puede usar para penetrar en una red de área local (LAN).** Si SNMP no se usa en una red, debe apagarse, porque además de crear una vulnerabilidad, consumirá el ancho de banda de red disponible y usará

innecesariamente ciclos de CPU. Un número significativo de herramientas de software puede escanear toda la red a través de SNMP, por lo tanto, los errores en la configuración del modo de lectura y escritura pueden hacer que una red sea susceptible a ataques.

5. **Bloque el correo no deseado y las ventanas emergentes del browser** Estas sencillas medidas de seguridad impiden la entrada de spam, malware y virus,

Seguridad en las redes privadas VPN

Una VPN (Virtual Private Network) es una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet. Las empresas suelen utilizar estas redes para que sus empleados, desde sus casas, hoteles, etc., puedan acceder a recursos corporativos que, de otro modo, no podrían. Sin embargo, conectar la computadora de un empleado a los recursos corporativos es solo una función de una VPN.

Como puede suponerse, a través de una VPN pasa información privada y confidencial que en las manos equivocadas, podría resultar perjudicial para cualquier empresa. Esto se agrava aún más si el empleado en cuestión se conecta utilizando un Wi-Fi público sin protección. Afortunadamente, este problema puede ser mitigado cifrando los datos que se envían y reciben. **Para poder lograr este objetivo, se pueden utilizar los siguientes protocolos que deben utilizarse al instalar una VPN:**

IPsec (Internet Protocol Security): permite mejorar la seguridad a través de algoritmos de cifrado robustos y un sistema de autentificación más exhaustivo. IPsec posee dos métodos de encriptado, modo transporte y modo túnel. Asimismo, soporta encriptado de 56 bit y 168 bit (triple DES).

PPTP/MPPE: tecnología desarrollada por un consorcio formado por varias empresas. PPTP soporta varios protocolos VPN con cifrado de 40 bit y 128 bit utilizando el protocolo Microsoft Point to Point Encryption (MPPE). PPTP por sí solo no cifra la información.

L2TP/IPsec (L2TP sobre IPsec): tecnología capaz de proveer el nivel de protección de IPsec sobre el protocolo de túnel L2TP. Al igual que PPTP, L2TP no cifra la información por sí mismo.
Parte de la protección de la información que viaja por una VPN es el cifrado, no obstante, verificar que la misma se mantenga íntegra es igual de trascendental. Para lograr esto, IPsec emplea un mecanismo que si detecta alguna modificación dentro de un paquete, procede a descartarlo. **Proteger la confidencialidad e integridad de la información utilizando una VPN es una buena medida para navegar en Wi-Fi públicos e inseguros incluso si no se desea acceder a un recurso corporativo.**

La empresa **ESET** experta en temas de seguridad evaluó diferente software para VPN, las tres que presentaron mejor desempeño en materia de privacidad y seguridad fueron **ExpressVPN, Nord VPN, Hotspot Shield Elite** y Private Internet Access. Cada una de estas cuatro VPN fueron las más completas para hacerle frente a cualquiera de los seis posibles escenarios de fuga de información.

ExpressVPN, PIA y NordVPN pasaron las pruebas para los seis tipos de fugas posibles, con la excepción de **NordVPN** que pasó cinco de las seis al fallar en la prueba de fugas de **WebRTC.**

Función kill switch
Según explica el informe, la función kill switch de una VPN protege a los usuarios de conectarse con una IP desprotegida una vez que se reestablece la conexión ante una eventual caída. En el caso de la prueba de esta funcionalidad, de las 12 VPN testeadas, NordVPN, Private Internet Access, ExpressVPN y Hotspot Shield fueron las únicas soluciones VPN que pasaron la prueba. Otro aspecto a destacar es que solo ExpressVPN tenía esta funcionalidad activada por defecto. Las demás requieren que se active de forma manual.

Protección ante URLs maliciosas
De las 12 VPN puestas a prueba, cuatro de ellas aseguraban ofrecer protección de sitios web maliciosos. En este sentido, luego de que se probó su desempeño con 25 sitios de phishing y 24 sitios que descargaban códigos maliciosos, se constató que F-Secure FREEDOME VPN, Hotspot Shield Elite y Private Internet Access aportaron cierta protección. En el caso de F-Secure FREEDOME VPN, bloqueó cerca de dos tercios de las páginas de phishing y más de la mitad de las páginas que dropeaban malware. En el caso de Hotspot Shield Elite, logró controlar más de la mitad de los sitios con phishing y cerca del 10% de las páginas que contenían códigos maliciosos. Por último, Private Internet Access no detectó ninguna de las páginas web que contenían phishing y apenas detectó un tercio de los sitios que contenían malware.

Seguridad en Wireless

¿Qué es una red inalámbrica?

Es una red que permite a sus usuarios conectarse a una red local o a Internet sin estar conectado físicamente mediante cables, sus datos (paquetes de información) se transmiten por el aire. Existen varios dispositivos que permiten interconectar dispositivos inalámbricos, de forma que puedan interactuar entre sí. Entre ellos destacan los puntos de acceso que controlan el acceso y las comunicaciones de usuarios conectados a la red y las tarjetas receptoras para conectar a la computadora personal, ya sean internas (tarjetas PCI) o bien USB

Consejos de seguridad para redes inalambricas

En los siguientes consejos aparece la figura de *el observador(intruso)*, como la persona de la que queremos proteger nuestra red.
Asegurar el punto de acceso por ser un punto de control de las comunicaciones de todos los usuarios, y por tanto crítico en las redes inalámbricas:

1. Cambia la contraseña por defecto.
Todos los fabricantes establecen un password por defecto de acceso a la administración del punto de acceso. Al usar un fabricante la **Cambia la contraseña por defecto.**
Todos los fabricantes establecen un password por defecto de acceso a la administración del punto de acceso. Al usar un fabricante la misma contraseña para todos sus equipos, es fácil o posible que *el observador* la conozca. ***Evita contraseñas como tu fecha de nacimiento, el nombre de tu pareja, etc. Intenta además intercalar letras con números.***

2. Aumentar la seguridad de los datos transmitidos Usa encriptación WEP(Wired Equivalent Privacy /WPA(WiFi Protected Access). Usa encriptación WEP/WPA. Las redes inalámbricas basan principalmente su seguridad en la encriptación de los datos que viajan a través del aire. El método habitual es la encriptación **WEP**, pero no podemos mantener

WEP como única estrategia de seguridad ya que no es del todo seguro. Existen aplicaciones para Linux y Windows (como AiroPeek, AirSnort, AirMagnet o WEPCrack) que, escaneando el suficiente número de paquetes de información de una red Wi-Fi, son capaces de obtener las claves WEP utilizadas y permitir el acceso de *intrusos* a nuestra red. **Las claves usadas por WPA son de 256 bits, el doble de los 128 bits usados por WEP**. Por lo que es mas seguro **el WPA**

Para poder entrar habría que tener acceso a la red protegida y hacer uso de ataques de fuerza bruta. Existe, eso sí, un agujero ya habitual en cifrados WPA, que también se encuentra en WPA2, a través del WPS (WiFi Protected Setup).

Visto lo anterior, cabría decir que para tener una red inalámbrica segura y óptima, deberemos de tener implementado el sistema de encriptación WPA2 con el cifrado AES, desactivando la opción WPS, para evitar posibles ataques. Y si disponemos de aparatos más antiguos no compatibles con el WPA2, aunque nos reduzca la velocidad de conexión, lo recomendable sería usar los cifrados TKIP + AES utilizando el modo mixto**.**

TKIP (*Temporal Key Integrity Protocol*) es también llamado hashing de clave WEP WPA, incluye mecanismos para mejorar el cifrado de datos inalámbricos

3. Ocultar tu red Wi-Fi: Cambia el SSID por defecto. Suele ser algo del estilo a "default", "wireless", "101", "linksys" o "SSID". En vez de "MiAP", "APManolo" o el nombre de la empresa es preferible escoger algo menos atractivo para *el observador*, como puede ser "Broken", "Down" o "Desconectado". Si no llamamos la atención de *el observador* hay menos posibilidades de que éste intente entrar en nuestra red.

4. Desactiva el broadcasting SSID, o identificador de la red inalámbrica. El broadcasting SSID permite que los nuevos equipos que quieran conectarse a la red Wi-Fi identifiquen automáticamente el nombre y los datos de la red inalámbrica, evitando así la tarea de configuración manual. Al desactivarlo tendrás que introducir manualmente el SSID en la configuración de cada nuevo equipo que quieras conectar.

5. Evitar que se conecten Activa el filtrado de direcciones MAC. Activa en el AP el filtrado de direcciones MAC de los dispositivos Wi-Fi que actualmente tengas funcionando. Al activar el filtrado MAC dejarás que sólo los dispositivos con las direcciones MAC especificadas se conecten a tu red Wi-Fi.

6. Establece el número máximo de dispositivos que pueden conectarse. Si el AP lo permite, establece el número máximo de dispositivos que pueden conectarse al mismo tiempo al punto de acceso.

7. Desactiva DHCP, asignación dinámica de direcciones IP.

Desactiva DHCP en el router o en el punto de acceso (AP). En la configuración de los dispositivos/accesorios Wi-Fi tendrás que introducir a mano la dirección IP, la puerta de enlace, la máscara de subred y el DNS primario y secundario. ***Si el observador conoce "el formato" y el rango de IP que usamos en nuestra red, no habremos conseguido nada con este punto.***

Para los más cautelosos:

8. Desconecta el AP cuando no lo uses.

Desconecta el punto de acceso de la alimentación cuando no lo estés usando o no vayas a hacerlo durante una temporada. El AP almacena la configuración y no necesitarás introducirla de nuevo cada vez que lo conectes.

9. Cambia las claves regularmente.

Por ejemplo semanalmente o cada 2 o 3 semanas. Antes decíamos que existen aplicaciones capaces de obtener la clave WEP de nuestra red Wi-Fi analizando los datos transmitidos por la misma. Pueden ser necesarios entre 1 y 4 Gb de datos para romper una clave WEP, dependiendo de la complejidad de las claves.

Mientras que en las redes cableadas es más complicado conectarse de forma ilegítima, habría que conectarse físicamente mediante un cable, en las redes inalámbricas donde la comunicación se realiza mediante ondas de radio, esta tarea es más sencilla. Debido a esto hay que poner especial cuidado en *blindar* nuestra red Wi-Fi.

Referencias

- André Goujon. (2012). *¿Qué es y cómo funciona una VPN para la privacidad de la información?*. 20 de agosto de 2019, de Welivesecurity Sitio web: https://www.welivesecurity.com/la-es/2012/09/10/vpn-funcionamiento-privacidad-informacion/

- Jesús Costas Santos. (2014). *Seguridad en Redes*. En Seguridad Informática (203-233). Madrid, España: RA-MA, S.A. Recuperado de: https://ebookcentral.proquest.com/lib/initesp/reader.action?docID=3228430&query=Seguridad%2Binform%25C3%25A1tica

- Kenneth C. Laudon y Jane P. Laudon. (2012). Seguridad en los Sistemas de Información. En Sistemas de Información Gerencial (310-318). EU: Pearson Educación.