OnRed

Internet - Television - Telefonía

“ Velocidad y entretenimiento sin limites ”

La Ciberseguridad es un tema apasionante, lo tengamos presente o no en nuestra vida digital.

Al vincular nuestra información personal y profesional con la computadora, el celular y dispositivos inteligentes IoT (TV, equipo de sonido, videocámaras, alarmas, refrigerador, aire acondicionado, etc) controlados desde Internet , estamos exponiendo está valiosa información a los delincuentes.

Ciberseguridad y Seguridad Perimetral para empresas, educación y particulares

Hoy te hablaré de los elementos básicos que debes tener en cuenta si deseas sobrevivir en este moderno mundo digital.

> ***Primero que nada es importante entender que debido a la complejidad en la “creatividad” de los Ciberdelincuentes, hoy en día NO existe una única solución para estar protegido.***

Erróneamente, muchas personas creen que un antivirus es suficiente; sin embargo, este no te protegerá de software malicioso o Malware que llegue a través de los navegadores de Internet, redes sociales, YouTube, juegos en línea, dispositivos IoT, entre otros.

Es necesario que tomes medidas complementarias.

¿Para Casa, escuela o Empresa?

Una PYME o un usuario hogareño también tienen la idea errónea de que debido a su tamaño, no son foco de estos ataques.

> *De acuerdo a las estadísticas, el 60% de las PYMES han experimentado durante los pasados 12 meses un ataque, robo o secuestro de su información.*

¿Recuerdas a los famosos que se han hecho más famosas por fotos o videos comprometedores?.

Ve por un café ya que estará entretenida la siguiente parte.

Iniciaremos definiendo las principales amenazas y terminología, luego te explicaremos cómo protegerte.

En su momento haremos la precisión de si aplica para un usuario en casa o eres encargado del área de TI en una empresa o incluso si haces "home office".

Aquí la terminología frecuente:

Ciberseguridad: Es una solución o Servicio para Proteger dispositivos (Servidores, PC's, Laptops, Tabletas, Celulares, dispositivos IoT) e información que "vive" en ellos.

Están conectados principalmente a Internet.

La idea es evitar el robo, manipulación o secuestro de la información empresarial o personal.

Virus. Es un software dañino, diseñado para entrar en un dispositivo, generalmente sin el conocimiento del usuario.

Se propaga a través de la red o correo electrónico, infecta a otras computadoras y puede causarte daños irreparables en el dispositivo.

Incluendo la información o afectando el rendimiento en general.

Códigos maliciosos o Malware: Son Aplicaciones o programas que tienen como fin infiltrarse en los dispositivos, funcionando de una manera silenciosa en la mayoría de los casos y poniendo en riesgo la información de los usuarios.

Diseñados para crear vulnerabilidades como puertas traseras, brechas de seguridad, robo de información y en general daños a información de la empresa y personal.

Las nuevas generaciones de Malware tienen componentes de **IA (Inteligencia Artificial)** y se activan con reconocimiento facial, hasta que encuentran a la persona correcta.

Como ejemplo **DeepLocker**.

Otros Malware se activan o transforman de acuerdo al perfil del portador y pueden esperar hasta encontrar a la victima con el perfil adecuado.

¿De miedo, no?. Parece ciencia ficción, pero es nuestra moderna realidad.

El Malware se "arma" y auto activa ante ciertas condiciones, como por ejemplo, si tienes tus contraseñas o datos bancarios guardados en los navegadores de internet o dispositivo. Desconfía de los sitios "gratuitos".

Recordemos que este es un articulo para principiantes y no ahondaremos en las características de cada componente; sin embargo se describen las más importantes. Al final, encontrarás una tabla con un resumen de las amenazas y la solución apropiada para hacerles frente.

> *El Malware a diferencia de los virus, puede llegar en porciones de diferentes correos o sitios de internet, esto con el fin de evitar la detección vía un antivirus.*

¿Quién o qué es un HACKER?

Es un experto en informática y programación. Su día a día es descubrir vulnerabilidades de sistemas operativos, aplicaciones, dispositivos y generar códigos con fines criminales.

Como entenderás, los hackers trabajan en el anonimato, a veces solos, pero generalmente en grupos o redes.

Los hackers dedicados al crimen se les llama también de **"Sombrero Negro"**, pero también existe su contraparte, los de **"Sombrero Blanco o éticos"**, cuya misión es igualmente descubrir vulnerabilidades y repararlas.

> *¿Has visto que tu Windows 10, IOS, OSX o Android piden tu permiso para actualizarse?*

Los de "Sombrero Blanco" seguramente encontraron una vulnerabilidad y la resuelven con esas actualizaciones.

Los de Sombrero Blanco generalmente trabajan en empresas de seguridad informática que se encargan de crear los Antivirus y Antimalware.

Créelo, es una guerra entre ambos bandos las 24 horas del día, los 365 días del año.

El Ramsomware y los BOTS

RAMSOMWARE. De la palabra en inglés RAMSON (Rescate). Es un software malicioso o Malware que tiene objetivos específicos como encriptar la información de un dispositivo y luego extorsionar al propietario para que por medio de un pago, generalmente en bitcoins, se libere o "rescate" la información por medio de una clave.

Este malware llega a través de archivos Word de contactos "confiables" o con temas o asuntos de correo que están relacionados con el trabajo o activad escolar o del día a día.

Ejemplo: "Proceso para el pago de su Factura". El Malware se instala en la computadora, examina los contactos y comienza a enviar correos usando el nombre del propietario del equipo infectado.

BOTNET. Este es un termino muy conocido en la redes sociales, un ejemplo ocurre cuando generas o contestas un tweet y no sabes si estás interactuando con un humano o un robot.

Son aplicaciones que tienen cierta inteligencia y responden ante estímulos, como palabras clave (frases) y que tienen una respuesta definida ante un tópico pre-establecido.

*Se forma de las palabras en inglés ro**BOT** y **NET**work (red).*

Un bot es una aplicación o script que ejecuta un comando permitiendo a un atacante tomar el control de dicho dispositivo.

Este dispositivo puede ser referido como un "**zombie**". Un grupo de estos dispositivos infectados son un BotNet.

El BOTNET es una variante de un Virus, definidos como **Troyanos**, su función es tomar el control de las computadoras infectadas, creando una red de "bots" para un fin malicioso.

Estas redes controladas de manera remota pueden ser incluso "alquiladas" a otros Cibercriminales y usadas para transmitir SPAM o ataques DDoS a sitios legítimos de internet.

También la idea es crear perfiles de personas falsos.

Cientos de millones de dispositivos en el mundo están infectados con bots y en control de hackers.

Los propietarios de estos dispositivos típicamente no experimentan ningún síntoma; sin embargo su dispositivo es utilizado para enviar correos basura (SPAM), incluyendo todos los contactos del dispositivo pareciendo que es un email legitimo.

Los bots adicional a enviar correo basura, envían ataques DDoS, crean perfiles falsos, también pueden robar la información confidencial o financiera del dispositivo que lo porta.

¿Qué es el SPAM, Phising y DDoS?

SPAM. Es correo Basura. Es un correo no deseado, suele ser publicidad de productos o servicios. Se genera principalmente por empresas que compran bases de datos de usuarios y las venden a otras empresas para comercializar sus productos.

También es generado por los BOTS o BOTNET, como se mencionó antes.

Si bien, el principio del SPAM es solo distribuir publicidad, también es usado para infectar con código malicioso, como Ramsonware o Phising al dispositivo o a otros dentro y fuera de la red.

PHISING. Si bien no hay una traducción exacta de la palabra, debes de entender este Malware como una Suplantación de identidad o Estafa (Fisher).

Utilizando un "contacto confiable" para hacerte creer que debes de abrir un correo o enlace de redes sociales.

Nuevamente el origen puede ser el SPAM o Redes Sociales.

> *Su objetivo es robar información confidencial de cuentas bancarias, tarjetas de crédito, contraseñas y toda aquella clasificada como sensible.*

DDoS. Ataque de negación de servicio distribuido (DDoS por sus siglas en inglés).

Se ejecuta por medio de BOTS o BOTNETs y la idea es utilizar tu computadora y la de cientos o miles de usuarios para generar un gran flujo de información o solicitud de ella a un sitio especifico.

Imagina que es como llevar miles o millones de manifestantes a las puertas de una institución pública o privada e impedir la entrada o salida de la gente e interrumpir el servicio.

> *Estos ataques coordinados tienen como fin "tirar" el servicio de un sitio de internet, como Bancos, Sitios de comercio en línea o páginas de algún organismo público o privado.*

Un sitio de internet colapsa cuando excede el número de visitantes para el cual fue diseñado el servidor que contiene la página.

Hay muchas amenazas que no hemos mencionado, pero estas son las principales.

¿Qué te parece hasta ahora toda la terminología de los Ciberseguridad?

¿Cómo Protegerte?

Ahora te describiré los mecanismos para poder proteger a tus dispositivos, si estás en casa o eres responsable del área de TI o soporte de una empresa.

Primero debes de recordar que tus dispositivos se conectan a internet y por lo tanto son vulnerables.

Tu modem de internet o Router (de tu proveedor de internet) generalmente ya viene con cierto nivel de seguridad y configuraciones básicas para protegerte.

Ejemplo: La **Clave de acceso WIFI encriptada o un Firewall.**

Utiliza Contraseñas Fuertes, que incluyan al menos una mayúscula, una minúscula, dos números, algún símbolo especial y al menos 8 caracteres de longitud . Ejemplo: Services4iT0%&

Si estás conectado a una red de datos 3G o 4G, estás completamente expuesto a un hacker o Malware.

¿Por qué una red pública es más vulnerable que la de tu casa u oficina?.

La respuesta con otra pregunta....

¿Dónde dejas con confianza tu cartera y reloj?, ¿En un Starbucks o en la sala de tu casa?.

Los intrusos actúan de manera anónima, generalmente a desconocidos.

Si eres el encargado del área de sistemas de una empresa, contratarás a un "policía cibernético" llamado FireWall UTM, como primera línea de seguridad.

Ya lo mencioné, una solución única para temas de seguridad no existe.

> *La Solución Recomendada es la suma de varias tecnologías.*

El malware puede llegar por una página web, correo electrónico, red social, compartir información como memorias USB, Bluethooth, wifi.

No olvides de la lista los dispositivos IoT.

Imagina, en tu oficina tienes un Firewall UTM que protege tu área perimetral, sin embargo no tienes antivirus y antimalware en los dispositivos de los usuarios.

Puede llegar el compañero que encontró una USB en la calle y tiene la inquietud de conocer el contenido, provocará un ataque interno que el Firewall UTM no detectará e infectará a toda tu red.

Mismo problema si el malware llega por un correo electrónico y una de los dispositivos no esta protegido.

Al final, te dejaré una tabla de las amenazas y como contrarrestarlas.

¿Qué tipo de usuario eres?

Ten en mente estos componentes para estar casi al 100% protegido (Nada es impenetrable).

Usuario Casero, Home Office o te guste trabajar en cafés internet.

1. **Un Antivirus.**
2. **Un Antimalware**
3. **Una VPN**

Usuario Corporativo que trabajar la mayor cantidad de tiempo en oficina, pero te conectas en casa o cafés internet.

1. **Un Firewall UTM (Seguridad Perimetral de la red corporativa).**
2. **Un Antivirus**
3. **Un Antimalware**
4. **Una VPN**

Antivirus:

No lo obvies, es el primer elemento de seguridad que debes de instalar y tener actualizado, desconfía de antivirus gratuitos.

Todas las computadoras están expuestas a "pescar" un virus mientras navegan en internet, utilizan aplicaciones o juegos de origen dudoso (piratas) o comparten información entre usuarios y dispositivos.

Es posible que tu laptop tenga antivirus, pero tu teléfono no y penetren por este último.

Si estás buscando un buen antivirus, "googolea" por ejemplo, algo similar a: "los mejores antivirus 2020".

Evita los anuncios y ubica aquellas referencias confiables de especialistas como **PCWorld.**

Antimalware:

Como lo comentamos, el software malicioso o malware esta en constante evolución y muchas veces supera al primer elemento de seguridad (antivirus)y no logra detectarlo.

Hay varias razones: La primera es que el malware esta llegando en porciones y en diferentes momentos, cuando esta completo se "arma" de maneras silenciosa en tu dispositivo y actúa.

¿Te ha ocurrido que comienza a llegarte mucha publicidad vía correo electrónico o Banners de Internet y tienes instalado un antivirus actualizado?.

La respuesta es que cuando navegaste en algún sitio, se instaló un código o plugin en tu equipo y esta monitoreando tu actividad, debido a que conoce tu correo, envía esta información para enviarte publicidad relacionada con tus gustos o preferencias.

Al igual que la recomendación para buscar un buen antimalware, "googolea". Uno que me ha dado una excelente experiencia es **MalwareBytes**.

VPN:

Es una Red Privada Virtual por sus siglas en inglés (Virtual Private Network).

Ya estas protegido con un antivirus y un antimalware, pero te gusta trabajar en Starbucks o cafés internet.... ¿es seguro?

La respuesta es NO. ¿Cuidas tus pertencias en un lugar público?

En una Red Pública, es muy posible que haya hackers buscando a personas que utilizan servicios bancarios o compras en línea y estén exponiendo su información bancaria y personal.

> **Los hackers tienen forma de poder realizar escaneos en la red y visualizar el tráfico, incluyendo tu información personal o de tu empresa.**

Te imaginarás que los fraudes bancarios están a la orden del día, precisamente por compras no reconocidas y esta equivale a miles de millones en todo el mundo.

Es un real dolor de cabeza para las instituciones bancarias y de crédito.

> *Una VPN sirve para poder rutear el tráfico de internet que entra y sale de tu computadora a un servidor seguro y encripta la información, de tal forma que es prácticamente imposible que alguien descifre lo que estas transmitiendo o recibiendo.*

Hay varias opciones, misma recomendación que para el antivirus y antimalware.

A la fecha llevo más de un año usando **NordVPN** y funciona excelente.

Cortafuegos o Firewall:

Solución de Hardware y/o software que es la primera línea de defensa de una red de dispositivos conectada a Internet.

Estas soluciones aplican a empresas pequeñas y grandes corporativos (**ver Firewall NG abajo**), pero puede ser una buena solución para residencias con una gran cantidad de dispositivos y efectivamente, es el primer punto de defensa que evite el tráfico malicioso hacia adentro y hacia afuera de tu red de datos o dispositivo.

Los primeros Firewalls de los años 90 sólo abrían o cerraban puertos de Internet, que son las "puertas" por las que las aplicaciones o servicios como Netflix, Spotify, correo, juegos en línea, navegadores de Internet que entran y salen del Módem o Router de Internet y llegan a tus dispositivos.

Existen fabricantes de Hardware y también de software para estas soluciones. Dos ejemplos son: Microsoft Windows, que incluye un firewall en el sistema operativo.

Los antivirus en algunos casos incluyen un Firewall.

Hay Hardware especializado que contiene software para realizar estas funciones.

Básicamente la diferencia entre ambos es que el primero solo te protege a nivel del servidor o computadora en donde este activo y el de HW/SW protege a nivel de toda la red.

UTM.

Es el acrónimo por sus siglas en Inglés, de **Unified Treath Management** o Administración Unificada de Amenazas.

> *Básicamente es software que constantemente se está actualizando de bases de datos mundiales relacionadas con diferentes tipos de Amenazas y por supuesto la solución para detenerlas.*

Este trabajo lo ejecuta un grupo de especialistas en Ciberseguridad y es una guerra literal entre el grupo de Hackers de sombrero negro y los de sombrero blanco.

Existen varios fabricantes de UTM en el mercado y dirigido a diferentes necesidades.

Los principales servicios que brinda un UTM son:

- Filtrado de Contenido, Analizan, detectan y detienen amenazas o políticas del administrador para el uso de aplicaciones no deseadas como Redes Sociales, YouTube, Netflix, etc.
- VPN. Explicado anteriormente.
- WEB Proxy. Administra el uso de los accesos a Internet.
- Antivirus. Explicado anteriormente.
- Antimalware. Explicado anteriormente.
- IDS/IPS, Sistema de Detección de Intrusiones/ Sistema de Prevención de Intrusiones por sus siglas en inglés.

FIREWALL UTM.

Como comprenderás de acuerdo a los conceptos anteriores, es una solución que combina las dos funcionalidades de Hardware y Software.

Está dirigida a empresas de pequeño y mediano tamaño.... ¿Porqué no a las grandes empresas?. Bueno, como lo comenté al iniciar el articulo, no hay una solución única para estar protegido.

Un **FireWall UTM** es una solución **TODO EN UNO** que funciona muy bien para organizaciones deseosas de protegerse a un precio justo y no tienen una gran cantidad de usuarios que ralenticen las aplicaciones que hagan uso de internet.

> *Son empresas que están preocupadas por evitar perdidas, secuestro o mal uso de la información.*

Estas organizaciones, también utilizan otros medio de protección para sus computadoras o servidores, como el respaldo en disco o cinta y lo mueven a otro lugar, siguiendo la regla del backup 3-2-1. Los tiempos de recuperación deben de ser considerados.

Recomendaciones para Firewall UTM

Si tu organización tiene un alto volumen de transferencia de datos e intercambio de información con internet, es posible que el Firewall UTM quede "corto", provoque lentitud y demerite el servicio y/o este dejando pasar amenazas a tu red aunque todo este actualizado.

Puedes realizar dos tareas antes de buscar otra solución, una es ajustar las reglas de acceso, es posible que Youtube, redes sociales, netflix u otros estén abiertos a todos los usuarios y esto cause la lentitud o que se estén enviando correos con archivos de gran capacidad.

Si las politicas están bien implementadas, existe un gran número de usuarios y los servicios del UTM están tomando mucho tiempo para atenderlos y siguen filtrándose amenazas, es muy probable que debas pensar en separar las soluciones.

No es un tema de marcas y modelos e ir con prueba y error, todas las organizaciones tienen requerimientos y necesidades diferentes.

Busca a una buena consultoría para realizar un levantamiento, antes de comprar alguna solución.

FIREWALL NG.

Firewall de Siguiente Generación por sus siglas en inglés (**Firewall Next Generation**).

Es común pensar que un Firewall de siguiente Generación es mucho mejor o más avanzado que un Firewall UTM.

Es cierto, pero no te confundas o te confundan, tampoco permitas que te vendan una cosa por otra.

Firewall NG esta hecho para solventar lo que un Firewall UTM clásico no puede y principalmente tiene que ver con la profundidad del análisis para la detección, prevención y Filtrado.

Un Firewall UTM con todos los componentes de Software no realiza un examen profucndo de los paquetes.

Estas son las principales razones por las que sigue llegando malware a la red local, adicional a aumentar el rendimiento y experiencia de los usuarios.

Recuerda que la información digital viaja en paquetes de datos "0s" y "1s".

Estos Firewalls NG están Orientados a realizar una inspección profunda de paquetes en la capa de aplicación (Layer 7).

¿Qué significa?

En términos simples es que antes de que la información llegue a la red LAN estará filtrada y segura, mucho más que con un Firewall UTM tradicional y menciono tradicional, porque algunos fabricantes incluyen esta funcionalidad de inspección profunda de paquetes en los nuevos modelos.

Siendo un poco técnicos:

Hay 7 capas en el modelo OSI que nos permiten conocer como viaja un paquete de datos desde la capa física hasta la capa de aplicación.

La diferencia principal entre los dos modelos de Firewalls ronda en el examen de los paquetes a nivel de capa (layer).

Un Firewall UTM generalmente examina en la capa 3 y 4 (Red y Transporte) y el **Firewall NG** lo hace en las mismas capas, pero adicional en la capa 7.

Hacerlo a nivel de capa 7 permite vincular los diferentes paquetes con la aplicación y de esta forma determinan la legitimidad de un paquete.

Lo sospechoso que no corresponda, se considera como amenaza.

A los Firewalls NG también se les denomina Firewall Stateful.

Precisamente con el fin de ofrecer un mejor rendimiento, algunos fabricantes separan los equipos y algunos de estos Firewall NG retiran las funcionalidades de Antivirus, AntiMalware y WEB Proxy.

Aquí la tabla prometida.

USO					
AMENAZA	**ANTIVIRUS**	**ANTIMALWARE**	**VPN**	**FIREWALL UTM**	**FIREWALL NG**
Virus	😊	😟	😟	😐	😟
Ramsomware	😟	😊	😟	😐	😊
BotNet	😐	😊	😐	😐	😊
Troyano	😐	😊	😟	😐	😊
Spam	😊	😟	😟	😐	😟
Phising	😐	😊	😐	😐	😊
DDoS	😐	😊	😐	😐	😐
Web Proxy	😟	😟	😟	😊	😟
Redes Públicas	😟	😟	😊	😊	😟
Simbología					
Casa			😊	Completa Funcionalidad. Requiere de Antivirus, Antimalware o VPN	
Oficina			😐	Cumple parcialmente requiere de Antivirus, Antimalware o VPN	
Escuela			😟	No tiene la Funcionalidad	

Amenazas de Ciberseguridad

CONCLUSIONES:

La moderna vida Digital implica entender las nuevas amenazas que ponen en riesgo la información Privada, de la escuela o Empresa.

Es muy sencillo solucionar, si se trata uno a decenas de usuarios, sin embargo se va complicando a medida que los usuarios aumentan y sus politicas o reglas se restringen.

El número de dispositivos, aplicaciones y lugares desde donde acceden los usuarios y por supuesto los sistemas operativos involucrados son otro elemento a considerar.

Recuerda, no hay una única solución, casí todos los clientes y casos son diferentes. Busca una ayuda genuina, tiene que realizar un levantamiento, entender a tu organización o caso y luego proponerte algo que se adapte a tus necesidades.